Digital Democracy: A Case Study of the U.S. Immigration Policy and Its Datafication as a Human Rights Abuse

William Smith / Florian Grolleau

4A-DD

2025

Contents

1 Introduction

After winning the 2024 presidential election, Donald Trump made the fight against illegal immigration one of his campaign priorities. Following his inauguration, tougher policies were implemented towards people residing illegally in the United States. Immigration and Customs Enforcement (ICE) carried out raids to arrest immigrants in the United States. According to a September 2025 article in The Guardian (which we would refer as Bhuiyan, 2025), ICE is working with the private company Palantir Technologies, which specialises in data analysis, to provide them with software and applications to collect personal data on people who may be in the country illegally, as well as facial recognition and geolocation capabilities via mobile phones. These practices carried out by ICE with the tech company Palantir have alerted many civic rights organisations to the risk of human rights violations against immigrants in the US (Bhuiyan, 2025).

One of the rights threatened by this new policy is the right to privacy and protection of personal data, which is the subject of this study. Digital democracy is the use of information and communication technology (ICT) and computer-mediated communication (CMC) in all kinds of media (e.g. the Internet, interactive broadcasting and digital telephony) for purposes of enhancing political democracy or the participation of citizens in democratic communication (Hacker & van Dijk, 2000). Respect for the right to privacy and the protection of personal data is a key issue in digital democracy, which opposes the possible abuse of data collection and digital surveillance. The use of personal data and surveillance by ICE and Palantir may threaten the rights to privacy and the protection of personal data, which are important principles of digital democracy.

1.1 Immigration policy context and the ongoing datafication background (2025)

In 2025, Donald Trump is elected in a politically polarised country. One of the themes of his political campaign is the fight against illegal immigration in the United States and the deportation of undocumented migrants. Numerous raids are carried out in American cities to arrest people who have arrived illegally. Especially in the southern states, where ICE claimed to detain almost 60,000 migrants in September 2025 (NBC News, Sept 2025). The new immigration policies become a source of partisan tension between Republicans who support the new Trump administration and their Democratic opponents. The arrests and the means used to carry them out spark a debate about human rights violations as it is a political issue that is expanding in scope, with an increase of 330% of ICE's detainees between October 2024 and September 2025 (MIP, October 2025). Surveillance tools and the collection of private data are being used as part of the policy to combat illegal immigration. Digital tools are increasingly being used to identify and arrest undocumented migrants. The right to privacy and protection of personal data, important principles of digital democracy, are not being respected.

The United States is a representative democracy, but the electronic surveillance carried out by immigration police is reminiscent of certain methods that describe what digital authoritarianism is. The fabric of digital authoritarianism is being woven through monitoring, datafication and AI, shrouding the public sphere and civic space in surveillance and control and challenging the notion that there is a meaningful distinction to be made between digital authoritarianism and digital democracy, meaning that it is only the political designation that distinguishes the two (Bhorat & Rauchbauer, 2023).

2 Research Question and Methods

Through these human rights potential violations strengthened by digital tools and particularly Palantir's contribution, rising concerns are emerging. In fact these violations are well defined by the Privacy Act of 1974, per example with the Medicaid data use scandal (AP News, July 2025). Those schemes of procedures within US immigration policies are enlightening the central role of data's use which leads us to a broader issue:

How could the Trump administration's policy of strengthening ICE's powers with the involvement of Palantir Technologies threaten the privacy rights and personal data protection of individuals in the United States?

Considering this main aspect of attack on privacy rights and personal data protection of individuals, one can assume that there is a privatization of the data collection, analysis and use

in the US as enlightened "We actually get to see Palantir providing these directions for very intense data surveillance," Lucal of Just Futures Law said. "As the administration is doing this work to consolidate systems of state surveillance even more than it already is, Palantir stands to profit from that."(Bhuiyan, 2025).

We also assume that the practices carried out by ICE correspond to forms of digital authoritarianism, without forgetting that the United States is a constitutional state with laws protecting individuals in the US. Moreover, it can be shown that those private companies (such as Palantir) which are signing multiple contracts with the government are sometimes left without a third part institutional surveillance authority as expressed: "Palantir has been used in Ice's day-to-day operations for data surveillance around deportations and that's been true for over a decade." (Bhuiyan, 2025).

"Now [with access to more federal databases] Ice can use this type of surveillance apparatus on anyone – not only anyone who is undocumented but anyone who this administration wants to criminalize and anyone who the administration wants to put under surveillance," said González of MediaJustice in 2025, who could be political opponents.

Finally, could we consider such government and private companies behavior as digital authoritarianism, and to some extent since it is targeting weak socio-economical actors mostly from the southern hemisphere are we witnessing an example of data colonialism? As defined by Couldry and Meijas in 2019, since the exploitation of these weak social groups helps to reinforce political dominance by achieving immigration policy objectives with some populist tendencies.

2.1 Methodology

For this study, we used various resources to explain the facts and hypotheses presented. The hypotheses were developed after reading press reports, including an article in The Guardian, which led us to choose the case of ICE and Palantir. To verify them, we read US laws on data protection and privacy, as well as scientific articles on digital democracy, in order to link our practical case to the theoretical principles of digital democracy. To verify the accuracy of the information from press reports, we checked other articles sharing the same information. We searched for government documents and research articles using Google Scholar and recorded the references from the various resources using Zotero.

3 Case Study Analysis

3.1 The role of private companies to serve the government expulsion policy

Private owned companies quickly positioned themselves as an unavoidable actor at the intercept between the growing place of data use and collection and the rise of massive surveillance and deportation as a political spearhead of Trump's presidency second term. Initial trigger is often considered as the collaboration between Palantir Technologies and the US government has resulted in government contracts worth approximately US$30 million for the creation of an application developed by Palantir called ImmigrationOS.

According to ICE, the tasks to be integrated into the application are to save time and resources in the selection and detention of 'violent criminals,' 'members of known transnational criminal organisations,' or migrants who have exceeded the validity of their visas (Limón, 2025). The software is being developed to collect data on immigrants who are in the United States without authorization or without a valid or expired visa, and to facilitate their deportation.

Various tools developed by Palantir have been used by US federal agencies since 2014, such as the facial recognition software developed by Clearview AI, which is used to identify undocumented immigrants (Bhuiyan, 2025).

Human rights advocates say that what is happening now significantly worsens the level of human rights violations, as it establishes a methodology of total social control aimed at maximising the effectiveness of immigration agencies in deporting immigrants and persuading them to leave US territory (Limón, 2025).

3.2 The legal considerations of the Palantir and U.S. government actions

On a legal basis multiple weaknesses and threats to human rights could be detailed. At first, an Amnesty International's report over the legality of Palantir actions was published in 2020 (the "Failing to do Right" report). This report consists of a call of Amnesty for Palantir of the urge of respecting human rights. Pointing the ICM technology provided by Palantir to ICE, Amnesty International proved its use in mass workplace raids proceeded by ICE agents.

Furthermore, in 2025, in an updated report Amnesty international again provided strong evidence of outcrossing violations of human rights. Palantir and ICE are using the so-called "Catch and Revoke" method (Amnesty, 2025) which consists of OSINT analysis supported by social media monitoring, visa status tracking, and automated threat assessment.

The US government responded quickly by legally legitimizing the whole operation using multiple laws such as the Presidential Executive Orders including EO 14159 and Executive Order 13773 (US government, 2025).

3.3 What could be the future of this cooperation?

In addition to the exterior protest regarding private companies involvement in ICE anti-immigration actions, another kind of protest recently arose: the resignation wave of former Palantir employees (NPR, 2025). Thirteen former engineers wrote an open letter accusing the company of deflecting from its original ethical aspirations.

"Big Tech, including Palantir, is increasingly complicit, normalizing authoritarianism under the guise of a 'revolution' led by oligarchs. We must resist this trend." (NPR, 2025)

Due to the heavy role occupied by Palantir's technologies nowadays, the US organizations (ICE, Border Patrol) remain substantially dependent. Moreover, those tools are extremely profitable for Big Tech companies: "Since Trump was elected, Palantir's share price has surged more than 200%." (Google Finance, 2025).

4 Conclusion

This study finds that ICE's work with Palantir Technologies and the Trump administration's crackdown on illegal immigration may threaten privacy rights and personal data protection in the United States.

The conclusions of the ICE and Palantir case have broader implications for the foundations of digital democracy. Digital democracy relies on transparency and the ethical use of digital technologies.

In the United States, the case between ICE and Palantir has alerted many American activist associations for the protection of rights and serves as a reminder that the use of digital tools may violate certain American laws, such as the Privacy Act of 1974.

5 References

Bhuiyan, J. (2025). Documents offer rare insight on Ice's close relationship with Palantir. The Guardian.

Bhorat, Z., & Rauchbauer, M. (2023). Decoding digital authoritarianism.

Couldry, N., & Mejias, U. A. (2019). Data colonialism.

Hacker, K. L., & van Dijk, J. (2000). Digital democracy.

Office of Privacy and Civil Liberties (2014). Privacy Act of 1974.

Limón, R. (2025). ImmigrationOS by Palantir. El País English.

NBC News (2025). U.S. immigration enforcement tracker.

Migration Policy Institute (2025). A new era of enforcement.

AP News (2025). Trump wants Medicaid used to check immigrant status.

Amnesty International (2020, 2025). Reports on Palantir.

NPR (2025). Palantir workers issue letter on Trump policies.