

The EU Screening Regulation and the Fight for Digital Privacy at the Border

Written by Sarah Barrie

Edited by Jip Aukes, final editing by Joey Trebing

Abstract

The increasing reliance on smartphones as digital archives at European borders poses severe fundamental rights challenges. The upcoming EU Screening Regulation compels Member States to conduct security checks that may involve digital data extraction. This article examines whether these practices can be reconciled with the privacy standards established by the Court of Justice of the European Union in the judgements *Prokuratuur* and *Landeck*. The article argues that reliance on outdated analogue frameworks or the legal fiction of asylum seekers' consent is untenable. The lawful implementation of the Screening Regulation requires robust national legislation that guarantees prior independent review to protect migrants' digital privacy.

Keywords: EU Screening Regulation, Right to Privacy, Digital Evidence, CJEU, *Landeck* Doctrine, Migration Law, Consent, Fundamental Rights.

Introduction

A smartphone is far more than an ordinary physical possession; it is a comprehensive digital archive which can contain a 'more or less complete picture' of a person's private life.¹ Consequently, when European border authorities access an asylum seeker's phone, they commit what the European courts classify as a 'serious interference' with the right to privacy.² While such intrusive measures legally demand 'particularly precise' legislation and clear procedural safeguards, the reality at EU borders frequently unfolds in the absence of a clear legal framework.³ The context of modern migration exacerbates this issue. Migrants frequently arrive at European borders without physical identification documents, leaving their smartphones as the primary, and often only, means for authorities to verify their identity or origin.⁴ This operational reality clashes directly with fundamental rights.

¹ HR 4 April 2017, ECLI:NL:HR:2017:584 (*Smartphone-arrest*).

² Case C-746/18 *Prokuratuur* ECLI:EU:C:2021:152; *Saber v Norway* (App No 45918/15) (ECtHR, 17 December 2020).

³ Case C-746/18 *Prokuratuur* ECLI:EU:C:2021:152, Case C-548/21 *Bezirkshauptmannschaft Landeck* ECLI:EU:C:2023:764.

⁴ European Migration Network, *Challenges and Practices for Establishing the Identity of Third-Country Nationals in Migration Procedures* 17 (EMN Synthesis Report, European Commission 2017); Evelien Brouwer, 'Uitlezen van smartphones in de asielprocedure – voor welk doel en met welk recht?' (2023) 8 *Asiel- & Migrantenrecht* 372 https://research-portal.uu.nl/ws/portalfiles/portal/277311203/2023_a_mr_08_artikel_evelien_brouwer.pdf accessed 26 February 2026.

The recently adopted EU-Screening Regulation requires Member States to conduct identity and security checks on undocumented migrants at external borders.⁵ In practice, these checks will likely involve the extraction of smartphone data. However, the Screening Regulation does not provide any specific, harmonized rules on how to lawfully extract and process digital data from mobile devices. This raises a pressing question: how can Member States implement the EU Screening Regulation and perform thorough border checks without systematically violating the fundamental rights of asylum seekers?

The fallacy of the analogue approach

For a while, border authorities across Europe have sought to fit the digital reality of smartphone data extraction to outdated, analogue legal frameworks. A striking illustration of this phenomenon occurred recently in the Netherlands. For several years immigration authorities relied on general powers of search and seizure to extract digital data from smartphones.⁶ This practice effectively classified smartphones as mere physical ‘luggage’ under traditional Dutch administrative law.⁷ This analogue reasoning is increasingly difficult to sustain. A modern smartphone is not a static physical container; it is a hybrid device which functions as a portal to the ‘Cloud’ and holds a vast array of interconnected personal data.⁸ By applying traditional search powers to these digital devices without regulating appropriate safeguards and procedures a serious gap in fundamental rights protection was created.

Recent European case law shows that national courts are increasingly rejecting these outdated practices.⁹ The highest Dutch administrative court (Afdeling Bestuursrechtspraak van de Raad van State) has recently dismantled the ‘luggage analogy’.¹⁰ The court ruled that extracting data from an asylum seeker’s smartphone without a sufficiently specific statutory basis and procedural safeguards is unlawful.¹¹

As early as March 2022, the UK High Court struck down the English immigration authorities’ ‘secret and blanket policy’ of seizing and searching mobile phones from asylum seekers,

⁵ *Staatscourant* (Dutch Government Gazette) 2025, 6909407, p. 1-3.

⁶ *Vreemdelingenwet* 2000, arts 55 and 59.

⁷ *Staatscourant* (Dutch Government Gazette) 2024, 19165, 9.

⁸ This distinction between data stored on the device and data located elsewhere (via the device acting as a ‘portal’) was already recognised as fundamental in criminal law in the *Smartphone* judgments; see HR 4 April 2017, ECLI:NL:HR:2017:584.

⁹ Evelien Brouwer, ‘Uitlezen van smartphones in de asielprocedure – voor welk doel en met welk recht?’ (2023) 8 *Asiel- & Migrantenrecht* 372 <https://research-portal.uu.nl/ws/portalfiles/portal/277311203/2023_a_mr_08_artikel_evelien_brouwer.pdf> accessed 26 February 2026.

¹⁰ ABRvS 3 April 2024, ECLI:NL:RVS:2024:1387; ABRvS 22 January 2025, ECLI:NL:RVS:2025:132

¹¹ ABRvS 3 April 2024, ECLI:NL:RVS:2024:1387; ABRvS 22 January 2025, ECLI:NL:RVS:2025:132

declaring the practice a clear violation of article 8 of the European Convention on Human Rights (ECHR).¹² Subsequently, in 2023, the German Federal Administrative Court (Bundesverwaltungsgericht) held that requesting an asylum seeker's access credentials to inspect data on their mobile phone was disproportionate and therefore unlawful under articles 7 and 8 of the EU Charter of fundamental Rights.¹³ These rulings underscore that outdated analogue legal frameworks are ill-suited to regulate the access to the comprehensive digital archives that exist within smartphones. That broader tension also appears in the case law of the CJEU.

Setting the benchmark: The CJEU and the *Landeck* doctrine

The Court of Justice of the European Union (CJEU) has significantly raised the threshold for digital privacy protection. This protection is based on articles 7 and 8 of the Charter of Fundamental Rights of the European Union, which guarantee the right to respect for private life and the protection of personal data.

In the landmark judgements *Prokuratuur*¹⁴ and *Landeck*¹⁵, the Court clarified the legal reality of accessing digital devices in modern times. The Court recognizes that a smartphone is not merely an object, but a device capable of revealing a highly detailed and intimate picture of an individual's private life. The extraction of data from these devices by public authorities qualifies as a 'serious interference' with fundamental privacy rights.¹⁶ Together, these cases show that access to smartphone data cannot be treated as an ordinary investigative measure but requires strict procedural safeguards and independent oversight under EU law.

To justify such an intrusive measure, the Court established strict conditions. The most important requirement created by the *Landeck* case is the necessity of prior review. In practice, this means that access to data on a smartphone must be subject to prior review carried out by either a judge or an independent administrative body.¹⁷ This review is essential to prevent arbitrary action by authorities and to ensure that all interferences with fundamental rights remain necessary and proportionate.

¹² *HM, MA, KH v Secretary of State for the Home Department* (High Court (Administrative Court), 25 March 2022) joined cases CO/4793/2020 and CO/577/2021.

¹³ BVerwG 16 February 2023, 1 C 19.21.

¹⁴ Case C-746/18 *Prokuratuur* ECLI:EU:C:2021:152.

¹⁵ Case C-548/21 *Bezirkshauptmannschaft Landeck* ECLI:EU:C:2023:764.

¹⁶ Case C-746/18 *Prokuratuur* ECLI:EU:C:2021:152; *Saber v Norway* (App No 45918/15) (ECtHR, 17 December 2020).

¹⁷ Case C-548/21 *Bezirkshauptmannschaft Landeck* ECLI:EU:C:2023:764, [50].

Moreover, the Court stresses that access to smartphone data must be based on a ‘clearly defined statutory framework’.¹⁸ This framework should specify when authorities are allowed to access the smartphone data and for what purposes they may do so. Even then, authorities may only access data that is strictly necessary for their investigation¹⁹ and they must inform the individual once doing so no longer jeopardizes the procedure.²⁰

The illusion of consent at the border

Member States face a difficult legal dilemma. While the EU Screening Regulation calls for rigorous identity and security checks, it does not provide the ‘particularly precise’ statutory basis that the CJEU explicitly requires for these intrusive measures.²¹ Border authorities therefore operate in a ‘regulatory vacuum’, where they attempt to meet the European security mandates without the necessary procedural safeguards in place.

To navigate this gap, authorities in certain Member States have turned to the asylum seekers’ ‘consent’ as the primary legal basis for accessing digital devices. A prime example is Belgium, where a 2017 legislative amendment granted authorities the power to request and examine asylum seekers’ digital data carriers.²² This system relies on the asylum seeker’s consent, which is inherently problematic in the context of border control.

According to the General Data Protection Regulation (GDPR), consent is lawful when it is freely given, specific, informed and unambiguous.²³ At the border, an inherent and severe power imbalance exists between a highly vulnerable asylum seeker and the national border authority. The Belgian court highlighted this vulnerability²⁴ by referring to the CJEU’s judgement in *F. v Bevándorlási és Állampolgársági Hivatal*, which recognized that consent given during an asylum procedure does not necessarily amount to ‘free’ consent.²⁵ Because asylum seekers may fear that their refusal to hand over their devices could affect their asylum claim, it becomes difficult to argue that handing over the device is truly voluntary. Using this

¹⁸ Case C-548/21 *Bezirkshauptmannschaft Landeck* ECLI:EU:C:2023:764, [98].

¹⁹ Case C-548/21 *Bezirkshauptmannschaft Landeck* ECLI:EU:C:2023:764, [79].

²⁰ Case C-548/21 *Bezirkshauptmannschaft Landeck* ECLI:EU:C:2023:764, [50].

²¹ EU Screening Regulation, arts 10–13.

²² Loi modifiant la loi du 15 décembre 1980 sur l’accès au territoire, le séjour, l’établissement et l’éloignement des étrangers et la loi du 12 janvier 2007 sur l’accueil des demandeurs d’asile et de certaines autres catégories d’étrangers.

²³ Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) OJ L119/1, art 4(11).

²⁴ Grondwettelijk Hof 25 February 2021, nr 23/2021.

²⁵ Case C-473/16 *F v Bevándorlási és Állampolgársági Hivatal* ECLI:EU:C:2018:36.



form of consent as a replacement for the independent *ex ante* review risks undermining core European data protection principles.

Conclusion

European border controls are becoming increasingly digital, yet the national legal frameworks have not developed at the same pace. Recent case law across Europe shows a growing resistance to outdated analogue frameworks and an overly broad reliance on asylum seeker's consent.

If Member States intend to use smartphone searches to implement the Screening Regulation, they will need national legislation that complies with the requirements set by the CJEU. This includes independent prior review and clear limits on what data authorities may access. Without such protections, the digitalization of border control risks undermining the privacy rights that the European legal order is designed to protect.

***Sarah Barrie** (2002, she/her) is a Dutch Master's student in Criminal Law at Vrije Universiteit Amsterdam, with strong interests in Migration, EU Law, and Juvenile Criminal Law. She plans to pursue an additional Private Law specialisation, aiming to comprehensively understand the intersection of individual rights and state powers.*



Bibliography

Table of cases

ABRvS 22 January 2025, ECLI:NL:RVS:2025:132

ABRvS 3 April 2024, ECLI:NL:RVS:2024:1387

BVerwG 16 February 2023, 1 C 19.21

Case C-473/16 *F v Bevándorlási és Állampolgársági Hivatal* ECLI:EU:C:2018:36

Case C-548/21 *Bezirkshauptmannschaft Landeck* ECLI:EU:C:2023:764

Case C-746/18 *Prokuratuur* ECLI:EU:C:2021:152

Grondwettelijk Hof 25 February 2021, nr 23/2021

HM, MA, KH v Secretary of State for the Home Department (High Court (Administrative Court), 25 March 2022) joined cases CO/4793/2020 and CO/577/2021

HR 4 April 2017, ECLI:NL:HR:2017:584 (*Smartphone-arrest*)

Saber v Norway (App No 45918/15) (ECtHR, 17 December 2020)

Table of legislation and official documents

Loi modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers et la loi du 12 janvier 2007 sur l'accueil des demandeurs d'asile et de certaines autres catégories d'étrangers. https://etaamb.openjustice.be/fr/loi-du-12-mai-2024_n2024006654.html

Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) OJ L119/1

Regulation (EU) 2024/1356 of the European Parliament and of the Council introducing the screening of third-country nationals at the external borders (EU Screening Regulation)

Staatscourant (Dutch Government Gazette) 2024, 19165, <https://zoek.officielebekendmakingen.nl/stcrt-2024-19165>

Staatscourant (Dutch Gouvernement Gazette) 2025, 6909407, <https://zoek.officielebekendmakingen.nl/stcrt-2026-25.pdf>



Vreemdelingenwet 2000, <https://wetten.overheid.nl/BWBR0011823/2026-02-28>

Secondary sources

Brouwer E, 'Uitlezen van smartphones in de asielprocedure – voor welk doel en met welk recht?' (2023) 8 *Asiel- & Migrantenrecht* 372 https://research-portal.uu.nl/ws/portalfiles/portal/277311203/2023_a_mr_08_artikel_evelien_brouwer.pdf accessed 26 February 2026.

European Migration Network, *Challenges and Practices for Establishing the Identity of Third-Country Nationals in Migration Procedures* (EMN Synthesis Report, European Commission 2017).