Biometric device locks – an invitation to law enforcement?

An analysis of EU limitations to the contentious police practice after the "Landeck"-Decision

*von Prof. Dr. Carsten Momsen und Miriam Süttmann**

Abstract

*Inzwischen ist es gängige Praxis der deutschen Polizei, Smartphones mithilfe biometrischer Daten zu entsperren. Geschieht dies durch Zwang, sind Rechtsgrundlage wie Rechtmäßigkeit jedoch umstritten. Die Bedeutung der Law Enforcement Data Protection Directive (EU-RL 2016/680), vom EuGH 2024 in seiner „*Landeck*"-Entscheidung präzisiert, erlangt in dieser Debatte (zu) wenig Beachtung. Denn auch die Einhaltung europäischer Minimalstandards wird gefährdet, wenn die träge deutsche Gesetzgebung sich fortentwickelnde Polizei-Taktiken in einem sich rasch wandelnden technologischen Umfeld nicht reguliert, insbesondere so lange Gerichte die missachteten Anforderungen nicht durchsetzen. Vor diesem Hintergrund versuchen wir nachfolgend eine Einordnung der kontroversen Entscheidungen des BGH (2 StR 232/24) und des OLG Bremen (1 OR 26/24) aus dem vergangenen Jahr im Lichte europäischer Standards.*

Nowadays, biometric data is routinely used by German law enforcement for the purpose of unlocking smartphones. However, when pursued by force, the legal basis and legality are contentious. The Law Enforcement Data Protection Directive (EU Directive 2016/680), which the ECJ clarified in its "Landeck" decision in 2024, provides a legal framework. The reluctance of German legislation to keep pace with rapidly evolving technological environments has the potential to compromise compliance with these standards. This is of particular concern when courts fail to enforce legal requirements, thus jeopardising civil liberties. Two decisions issued by the Federal Court of Justice (BGH, 2 StR 232/24) and the Higher Regional Court of Bremen (OLG Bremen, 1 OR 26/24) in the previous year were met with great controversy. As demonstrated below, these critics find themselves in alignment with the requirements imposed by EU regulations.

I. Introduction

The central role mobile phones play in everyday life – used to chat, store photos and documents, search the internet, access emails or cloud storages – evidently makes them a target for law enforcement. In the past, accessing the stored information could be difficult, when devices were password protected: Since *Nemo Tenetur* prevents obtaining the password from the user through coercion, police had to hope to find it somewhere in writing. Otherwise, they would have to crack open the device themselves – which would be a lengthy and costly process.[1]

A much easier way opened up with the spread of fingerprint sensors since the launch of the Apple iPhone 5S in 2013: Suddenly law enforcement could bypass the PINs in many cases by placing the user's finger onto the sensor, often with brute force.

Since then, it has become standard police practice to unlock phones using biometric features, such as fingerprint-, face- or iris-scans: A German Police officer recommends on an independent police journal's online blog, to *"assist [the phone user] in unlocking their phone, if needed by force"*, if they are present.[2] Meanwhile, grassroots groups, protest organizers and human rights organizations are warning citizens "*to not have face or fingerprint lock on your phone, as the police can use those to unlock your phone without your consent*"[3].

The slow rate at which procedure codes adapt to technological change enables law enforcement to exploit loopholes and a lack of regulation, resulting in serious infringements of sensitive fundamental rights. Therefore, the rulings of high courts such as the *European Court of*

---

* *Carsten Momsen* is Professor for "Comparative Criminal Law, Criminal Procedural Law, Corporate Criminal Law and Environmental Criminal Law" at the Department of Law of the Free University Berlin, *Miriam Süttmann* is a member of his team. The following analysis was first presented as part of the Webinar "Police Access to Digital Devices: Where Are the Limits? Reflecting on the Landeck case C-548/21 and beyond" by Fair Trials, 3.12.2025, and further develops an expert opinion provided to the German Judges Association (Deutscher Richterbund) in 2018, published in modified form as *Momsen,* DRiZ 2018, 14.

1 Through trying out passwords (generally considered admissible, *Hegmann*, in: BeckOK-StPO, 57. Ed. (updated on 1.1.2026), § 110 Rn. 19; critical *Brodowski/Eisenmenger*, ZD 2014, 119 (123)), or through technical circumvention, as regulated in § 100b StPO. The latter is not popular, as statistics show, likely because it is too resource-intensive in the majority of cases, Bundesamt für Justiz, Übersicht Telekommunikationsüberwachung für 2022 (Maßnahmen nach 100b StPO), available online: https://bit.ly/4b7SaxQ (last accessed 10.1.2026).

2 *Weingarten*, KSV Polizeipraxis, available online: https://bit.ly/46BtbSk (last accessed 3.12.2025).

3 Quote from the initiative Gofilmthepolice by KOP (Kampagne für Opfer rassistischer Polizeigewalt), available online: https://bit.ly/4bncDA2; other examples are: Bündnis Widersetzen, available online: https://bit.ly/4r8EubR; Demo101, available online: https://bit.ly/4sbbKRn; Migrantifa Berlin, available online: https://bit.ly/4uiKnGr (all accessed on 3.12.2025).

Justice (ECJ) are becoming increasingly important in safeguarding citizens' rights.

II. Fundamental rights and EU minimum standards – the directive 2016/680 and Landeck

Authorities extracting information from devices in the EU are bound by Art. 7 and 8 of the Charter of Fundamental Rights (CFR), which guarantee the right to respect for private life and the protection of personal data. The minimum requirements for the processing of personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences are further specified by EU directive 2016/680 – also known as the *Law Enforcement Data Protection Directive*.[4]

In October 2024, the ECJ clarified in its *Landeck*-ruling[5] the limits and requirements the directive imposes on law enforcement's access to personal phones. Due to the sensitive nature of the stored data stored, including biometric information, personal recordings, photographs, cloud keys, health data and business secrets, which can be used to create movement or personality profiles, the court declared that any *attempt* to access phones and bypass locking measures seriously interferes with the fundamental right to privacy and the protection of personal data.

While not entirely precluded, access to mobile phone data is only allowed under high requirements: It must be based on a suitable enabling provision and guided by the principles of data minimization and proportionality. The respect of these principles is to be guaranteed by prior review by a judge or an independent administrative body. The ruling establishes that the severity of the offence under investigation is an essential factor in evaluating the proportionality of a measure. However, the court concluded that the directive should not be interpreted as limiting investigative powers to serious crimes, as this would unduly limit law enforcement authorities and undermine the objective of establishing an area of freedom, security and justice within the EU.[6]

III. Current (il)legal practice in Germany

As we will see, the German practice clearly falls far short of meeting these standards. Several times since 2017 courts had to position themselves on the admissibility of obtained information.[7] Points of contention are a possible conflict with *Nemo Tenetur*, as well as whether the German Code of Criminal Procedure contains a provision fit to enable the measure. While the practice doesn't necessarily directly violate the *Nemo Tenetur*-Principle, it still interferes with free will: Access to information is gained against the defendant's manifested will and encroaches therefore upon their freedom to store and provide personal data as they please. A legal basis would need to reflect this dimension.

In Germany, concerns regarding the legal foundation pertain to the fact that the German Code of Criminal Procedure – to this day – has not specifically regulated the forced unlocking of devices through biometric features. In line with *Landeck*, German jurisprudence recognizes that biometric unlocking by force cannot be based on general investigative authority. Does the measure therefore have no legal basis, rendering it illegal? Or could it be based on one of the existing provisions, and if so, what would the application require?

In identifying a legal foundation within the present Code of Criminal Procedure, three different approaches have been considered by the courts: Section 81a, that allows the physical examination of the accused, Section 81b, that allows the collection of photographs and fingerprints of the accused and Sections 94 ff., allowing and regulating infringements of the right to privacy, such as through searches, seizures of digital mediums, phone surveillance etc.

1. Section 81a

In 2017 a lower-level court ruled[8] that fingerprint extortion could be based on section 81a, regulating the physical examination of the accused. The application of Section 81a would be attractive to investigative bodies because the measure is subject to relatively lower requirements. Notably, it is not linked to serious offences. However, this understanding is now generally rejected. Rightfully so – measures under that section are reserved for the examination of the physical constitution, not the retrieval of data through physical features.[9]

2. Recent judicial practice: Section 81b

The prevailing judicial practice in Germany is such that law enforcement officials are authorized to unlock smartphones through fingerprint scans on the basis of Section 81b, which stipulates the collection of photographs and fingerprints of the accused.

Post-*Landeck*, two decisions by a Higher Regional Court (*OLG Bremen*) and the *Federal Court of Justice* (*BGH*) have upheld this reasoning,[10] that in two aspects seems to severely misinterpret both the law and the *ECJ*'s ruling: First of all, stating that the legality of accessing the phone can be evaluated separately from the search of the phone.

---

4 Directive (EU) 2016/680 Of The European Parliament And Of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

5 *European Court of Justice*, 4.10.2024 – C-548/21 (Landeck), available online: https://bit.ly/4cvqzsP (last accessed 4.3.2026).

6 *ECJ*, Landeck (fn. 5), para. 97. In agreement with the "German Jurists' Conference" (Deutscher Juristentag), see *Wahl,* eucrim 3, 2024, 189 (191).

7 *BGH,* NStZ 2025, 560*; OLG Bremen*, NJW 2025, 847; *LG Ravensburg*, NStZ 2023, 446; *AG Baden-Baden*, Beschl. v. 13.11.2019 – 9 Gs 982/19 (juris); *AG Verden*, 9a Gs 800 Js 15636/17 (2373/17), Beschl. v. 27.6.2017 (not published).

8 *AG Verden* (fn.7*)*.

9 *Momsen,* DRiZ 2018, 14 (15).

10 *OLG Bremen,* 1 OR 26/24 and *BGH,* 2 StR 232/24, fn. 7.

Secondly, concluding that the scope of Section 81b extends to unlocking smartphones by placing the fingerprint on the sensor, thereby disregarding the logic upon which annex powers are predicated.

a) Two measures – or just a prelude?

Both the *OLG Bremen* and the *BGH* recognize Landeck as a landmark ruling.[11] Still, both courts concluded that accessing the device and processing/storing the information are two separate measures that can be assessed separately and find their legal basis in different provisions. "Processing the data is a *separate, subsequent measure* to the unlocking and can be assessed independently according to the rules that apply to it."[12]

This contradicts a key aspect from the *Landeck*-ruling. The *ECJ* was very clear that the directive also applies to operations taking place prior to the processing itself – such as a processing attempt. The objectives of the directive, to ensure a high level of protection of the personal data of natural persons and their right to determine who has access to personal data, would be undermined by a narrow interpretation.[13] The directive does not merely protect the data itself, it also protects the safety mechanisms set in place to guard the data. Even if the intention behind unlocking a phone was merely to identify a person as the owner, the directive would still apply, since breaching the security mechanism is an intermediate goal. Whether or not further processing is intended is inconsequential.

The legal basis permitting access to the device therefore needs to be fit to protect against the extent and intensity of smartphone access *and* impose correspondingly high barriers to intervention. Moving beyond a superficial approach that focusses on the use of biometrics, the actual substance of the investigative measure comes to light: A prelude to the use of and access to data. Unlocking the device is a necessary preparatory or accompanying measure to searches of the device, chats, cloud storage, etc.

It is recognized, that accompanying legal measures – so-called annex-measures – intended to enforce the primary measure, can be based on the provision allowing the primary measure, if they are typically connected and are suitable, necessary and proportional with regards to the purpose of the primary measure.[14] The constitutional requirement of legal reservation is satisfied if the accompanying measure is so typical and subordinate that it corresponds to the objective intent behind the primary measure.[15] This concept results from the circumstance that many (primary) measures will have to be carried out against the will of the person concerned.

For example, an apartment search may involve breaking down the front door.[16] Now if a police officer uses my finger as a crowbar to break down the digital door to my smartphone –could this be treated as an annex to the subsequent search of my device?[17]

b) Scope of section 81b

It might seem obvious that section 81b is not a suitable basis for a device search that needs to overcome security mechanisms. The provision states that "Photographs and fingerprints of the accused may be taken, even against his or her will, and measurements may be made of the accused and other similar measures taken with regard to him or her insofar as is required for the purposes of conducting the criminal proceedings or for the purposes of the police records department."[18]

Nonetheless, both *BGH* and *OLG Bremen* argue that biometric unlocking can be based on the provision for taking fingerprints *for the purpose of conducting the criminal proceedings*, claiming that the broad wording allows the use of fingerprints for any and every purpose, as long as it suits the investigation.[19] The argument ties to the creation process, during which the scope of the provision was deliberately kept open to encompass technological advancements.[20]

This understanding disregards a key point: While the legislator opted for a technology-unrestricted understanding, this does not absolve it from the necessity to limit the scope to measures that align with the purpose of determining physical characteristics and conducting biometric/dactyloscopic comparisons – which the unlocking of a phone clearly goes beyond.[21] *For the purpose of conducting the criminal proceeding* is not sufficiently limiting.[22] After all, any police measure supposedly serves in some way the purpose of investigating crimes.

Furthermore, such a broad understanding of Section 81b does not adequately consider the impact of unlocking a phone on the right to privacy. While the *OLG Bremen* correctly points out that the German Constitutional Court considered the hidden, secret infiltration of information systems a particularly severe infringement (para. 17), the argument that openly accessing a secured device interferes less with fundamental rights is inaccurate. The Constitutional Court stated that an intense interference, comparable to the surveillance of the home, is given with any access to the data stored on personal devices.[23] Due to its

11 However, the higher regional court notably does not even recognize the applicability of the Law Enforcement Data Protection Directive on the unlocking of phones, *OLG Bremen* (fn. 7), para. 17.

12 "Das Auslesen des Mobiltelefons als Ziel der Entsperrung ist eine dem Entsperren nachfolgende Maßnahme, die selbstständig an den für sie geltenden Regeln gemessen werden kann." *BGH* (fn. 7) para.65, emphasis added.

13 *Landeck* (fn. 4), para. 74, 75.

14 *BGH,* NJW 2001, 1658 (1659); *AG Hamburg,* StV 2009, 636.

15 Extensively *Ziemann,* ZStW 2018, 762; *AG Hamburg* (f. 14), 637.

16 *Henrichs/Weingast,* in: KK-StPO, 9. Aufl. (2023), § 105 para. 14a.

17 *LG Ravensburg* (fn. 7); critical *Horter*, NStZ 2023, 446 (448), since forceful biometric unlocking requires the „use" of the human body.

18 Translation of the German criminal procedure code by *Dufjet/Ebinger/Müller-Tostin/Mahdi/Reusch*, published https://bit.ly/4rbLwfW (accessed on 30.11.2025).

19 *OLG Bremen* (fn. 7), para. 13, *BGH* (fn. 7), para. 62.

20 *Rottmeier/Eckel*, NStZ 2020, 193 (195).

21 *Ruppert,* StV 2025, 565 (565), see also *Momsen* (fn. 9), p. 15.

22 Unless the era of absolutist (investigative) power as seen in the 18th and 19th century not come to an end after all? *Ziemann*, ZStW 2018, 762 (773).

23 *BVerfG,* NJW 2016, 1781.

intensity and the often highly personal nature of the data stored on an information technology system, it compares the severity of the intrusion to that of a (secret) intrusion into the sanctity of the home. The differentiation between hidden and open measures should be understood as an emphasis on transparency and ensuring access to judicial review in these cases, since this is limited in the case of hidden access. This consideration does *not* suggest that the right to privacy is less affected by other, open access to protected device data, given that this also enables comprehensive monitoring of the system's use and reading of its storage media against the manifested will of the user.

As Cyber-investigations expert *Felix Ruppert* pointed out: Section 81b offers no protection against the extent and intensity of smartphone access, nor does it impose correspondingly high barriers to intervention. This comes as no surprise, as the regulation was never intended to interfere with fundamental IT rights. The fact that it is unsuitable for this purpose is a logical consequence.[24]

Forcing the unlocking of a device can also not be considered an annex to a measure under section 81b, since bypassing the device lock is the focus of the measure, not just enabling or accompanying a biometric (dactyloscopic) examination. Assuming otherwise would be akin to considering an apartment search to be a mere extension of breaking down the front door.

3. Scope of section 94 ff., 110 – annex to the examination of electronic storage media?

Now what happens if we switch to an understanding that moves beyond the use of biometrics to the actual intended goal – the securing of the data. Could it be based on Section 94 ff., allowing the searches of objects, including digital documents, of the suspect, and section 110 regulating the examination of documents and electronic storage media and of data stored with cloud providers?

This understanding is implied as an alternative in the *BGHs* decision. Considering the possibility of a judicial review requirement under *Landeck*, the court states that this would be met by the issued warrant allowing the apartment search, since the search was specifically intended to locate mobile phones.[25]

This approach seems plausible at first glance. However, it disregards that there is a significant difference between accessing openly accessible documents and digital storage, as opposed to those *consciously secured* through security measures, such as passwords. The intensity of the measure is not an effect of the use of biometrics, but that the system is "hacked" by brute force – in any form an intense breach to the right of privacy.[26] As the legislators' considerations regarding section 100b show, the key difference lies in the direct impact on the fundamental right to informational self-determination when accessing a secured device against the *manifested will* of the user.[27]

This dimension is not reflected in the scope of sections 94 ff., 110, because it was not taken into consideration by the legislator. Therefore, accessing and searching a device by unlocking it through biometric measures cannot be seen as a mere negligible annex, and based on these provisions.

IV. Alternative: Section 100b?

Section 100b on the other hand does allow encroachment on the scope of protection of the fundamental right to integrity and confidentiality of information technology systems as an independent manifestation of the right to privacy. It legitimizes the technical circumvention of device protection without the knowledge of the user to collect stored data. But the requirements are high: The suspicion of a severe crime from a specified catalogue, the graveness of the offence in the individual case, and the heightened significance of the infiltration for the investigations. The search is subject to strict procedural requirements and must be documented.

Of course, the measures we are discussing aren't identical: The circumvention of security measures does not take place by technical means, and not *without the knowledge* – but "just" against the will of the user. However, the objective of the intervention is comparable – and, arguably, so is the intensity of the interference with the right to privacy, since the search also enables comprehensive monitoring of the system's use and reading of its storage media. Therefore, while the wording does not allow direct application in the case of accessing a device through biometric measures, the analogous application of the standard lies at hand.[28]

One might argue that the strict provisions of Section 100b regarding judicial review, documentation, and restriction to a catalogue of severe crimes only serve to mitigate the hidden nature of online searches. However, this distinction is not as clear-cut as it seems, since it is common practice to force biometric unlocking on the spot, thereby also obstructing prior judicial review.

In any case, it is the legislator, not the courts, who must carve out these distinctions. That is the only way to ensure compliance with fundamental laws and the Law Enforcement Data Protection Directive, as set out in *Landeck*.

V. Conclusion: Regulation, until then inadmissibility

Current practice is shaped by significant uncertainty surrounding the requirements for breaches of security measures designed to protect the data on mobile phones – devices that store the most intimate information. The fact that, despite almost a decade of debates, there have been

[24] *Ruppert*, LTO, https://bit.ly/3MNoUVc (accessed on 30.11.2025).
[25] *BGH* (fn. 7), para. 73.
[26] This understanding is a continuation of the argument against brute-force-„hacking" by trying out passwords made by *Brodowski/Eisenmenger* (fn. 1), p. 123.
[27] *Momsen* (fn. 8), p.16.
[28] *Momsen* (fn. 8), p. 16-17.

no legislative efforts, is concerning.[29] Even more concerning is that German courts keep approving of this, in direct contradiction to ECJ case law and in disregard of the importance of the right to privacy. By abandoning procedure codes and making all means available for the purpose of investigating crime[30] the courts are exceeding their authority and eroding EU standards. The only true solution to this worrying trajectory is a legislative one: Either the broadening of the scope of section 100b, or the creation of an appropriate provision that takes into consideration fundamental rights as specified by *Landeck*. Until then, until there is clarity on the legal basis and procedure, courts must rule that any evidence obtained through forced biometric unlocking is inadmissible.

[29] Hopes that the *ECJ*'s decision would prompt the legislator to act, see *Wahl* (fn. 6), have not been fulfilled.

[30] *Schneider,* NStZ 1999, 388 (389), *AG Hamburg,* StV 2009, 636 (637), *Ziemann*, ZStW 2018, 762 (773).