*Human Interaction and Emerging Technologies (IHIET-AI)*, Vol. 201, 2026, 358–368
https://doi.org/10.54941/ahfe1007190

# A Field Study on Data Protection and IT Security in AI-Supported Cashierless Stores

**Kai Lückhoff, Marko Schuba, Tim Höner, Sacha Hack, and Georg Neugebauer**

Aachen University of Applied Sciences, Aachen, Germany

## ABSTRACT

The retail sector is undergoing significant transformation driven by digital technologies. One notable development is the cashierless store, where customers can shop and leave without going through a traditional checkout, with automatic billing enabled by cameras, sensors and AI. For retailers this system not only increases efficiency but also provides valuable data on customer behaviour, which can be leveraged for marketing. Despite these advantages, concerns about data protection and IT security persist. In particular, the use of skeleton-based tracking raises privacy issues. This paper presents an analysis of the technical fundamentals and data protection challenges of cashierless store systems, taking German supermarkets as an example. The results show that data protection is often inadequately implemented and that customers are hardly informed about data collection.

**Keywords:** IT security, Data protection, Cashierless store, Artificial intelligence, Field study

## INTRODUCTION

The retail sector is undergoing profound structural change. This is being driven largely by digital technologies. Applications such as online ordering, click & collect, self-checkout, and mobile payment methods have become firmly established as part of the shopping experience and are now taken for granted by many consumers (MWIKE 2024). The systems are changing not only operational processes, but also expectations in terms of convenience, speed, and flexibility.

This dynamic also affects the food retail sector. Typical characteristics of this sector are short dwell times, high customer frequency, low margins, and strong demand for freshness. Consumers expect uncomplicated processes, short waiting times, and a shopping experience that can be smoothly integrated into their everyday lives.

In Germany, where this study was conducted, the food retail sector is facing increasing challenges. According to GTA (German Trade Association 2024) around 120,000 retail jobs could not be filled in 2023. This staff shortage is particularly acute in the food retail sector, which accounts for around 60% of brick-and-mortar retail sales (EHI 2023). Digital systems might counteract those staff shortages while at the same time providing

Received November 17, 2025; Revised December 28, 2025; Accepted January 7, 2026; Available online April 1, 2026

information useful for marketing and meeting customer expectations in terms of speed and convenience (EHI, 2024; MWIKE, 2024). One example is the cashierless store which allows customers to take products from the shelves and then leave the store without going through the checkout process. Billing is automated in the background (Pettigrew, 2025).

Consumer studies show that digital solutions are becoming increasingly accepted. A survey by (Bahr, 2022) cites the elimination of queues as the most important advantage of cashierless systems. Of the approximately 1,000 respondents, 84% saw this as a decisive added value. Another study conducted in Germany emphasizes the desire of many consumers to combine the speed and convenience of online shopping with the immediate availability of brick-and-mortar stores, combining digital ease with physical presence (MWIKE, 2024).

Regardless of the advantages that cashierless stores offer to customers and retail companies, key questions about European data protection law and IT security remain unanswered. This is because some of the data collected is particularly sensitive, such as biometric movement profiles created by skeleton-based tracking. In this context, data protection experts warn that current cashierless shopping concepts are not always compatible with applicable European data protection regulations, as customers have little insight into what data is collected and how long recorded images, for example, are stored or evaluated (Sluiter, 2022). In addition, the processing of large amounts of data always carries with it potential risks of abuse, for example through system errors, inadequate protective measures, or cyberattacks (Gärtner, 2024).

This paper deals with data protection and security issues arising from the use of cashierless shopping systems. It examines how such systems work technically, what data is collected and stored, and whether this procedure is compatible with the requirements of the General Data Protection Regulation (GDPR). The paper is based on a combination of literature-based analysis and empirical research: field observations in stores, a standardized customer survey, and a qualitative expert interview. The combination of these perspectives enables a multi-perspective view of the security-related, data protection, and social challenges associated with the use of cashierless systems.

## BACKGROUND AND RELATED WORK

Cashierless store systems are based on an advanced form of self-checkout. The technology allows for fully automated and contactless identification as well as video recording of customers (Reuter, 2024). Modern cashierless store models are increasingly relying on motion detection techniques (Sluiter, 2022). Of particular importance is skeletal gait analysis, in which a person's body structure and movement patterns are recorded and evaluated using cameras and AI systems (Reuter, 2024). The aim is to identify individuals in the store based on their gait pattern without resorting to facial features. This infrastructure is often supplemented by shelf sensors and cloud-based analysis systems, which together enable smooth, cashierless shopping (Reuter, 2024; Gärtner, 2024).

In cashierless stores in Germany, depending on the size of the store, around 200 to 500 cameras are installed on the ceiling along the aisles, supplemented by weight sensors in the shelves (Reuter, 2024). The interaction of cameras and sensors enables a three-dimensional model of the store space, in which all customer movements are recorded and can be traced if necessary. Every item that a customer takes from the shelf or puts back is digitally registered (Gärtner, 2024; REWE, 2022). For customers, this means: enter, shop, leave. After leaving the store, the purchase is automatically billed via an app, without the need for a conventional checkout process (REWE, 2022). According to the retailer, only the products that are taken or put back are recorded in a “data-minimizing” manner that claims to work without recording biometric characteristics (Gärtner, 2024). Tracking of customers is based on their physique and movement patterns, which the privacy policy explicitly refers to as a “schematic representation of your bone structure” (Reuter, 2024). Despite this wording, the retailer emphasizes that this does not involve biometric data processing. The technology provider of cashierless stores states that the system follows a privacy-by-design approach, as cameras generate 3D models of customers and track their movements without capturing their faces in sharp detail (Franken, 2021; Reuter, 2024). Classic biometric features are deliberately avoided. Instead, the system works with abstracted skeletal data, which is represented by a randomly generated ID (Franken, 2021).

Experts such as biometrics expert Jan Krissler (cited by Reuter, 2024) disagree with this assessment, arguing that the recording of physical characteristics is the epitome of biometrics and that it is irrelevant whether a 3D model is calculated from this data or whether the data is pseudonymized.

## General Shopping Process

Shopping in cashierless stores is clearly structured, from entering the store to recording movements and products to final billing. Note, that the process can be slightly different depending on whether the customers are using their retailer app with a registered account or not.

**Initialization upon entry:** As soon as a person enters the store the cameras register a new body silhouette. An anonymous identifier is generated from the video stream, essentially a numbered skeleton model that represents the customer without a name; as mentioned, no facial recognition takes place (Franken, 2021).

**Continuous tracking:** As the person moves through the store, AI-supported camera systems continuously track their position. A digital twin of the store helps to locate every movement spatially. This makes it possible to recognize which shelf a customer is standing in front of and where he or she is reaching (REWE, 2023). A key biometric feature used by such systems is a person’s individual gait. This is based on specific body proportions and movement patterns, is recognizable even from a distance, and is difficult to manipulate (Parashar et al., 2023). Modern systems in cashierless stores make use of this principle by relying on the analysis of movement dynamics instead of facial recognition (Reuter, 2024). This involves the use of algorithms from the field of pose estimation and object tracking, which continuously analyse a person's posture and movement and assign them to the created digital identity (Teepe et al., 2022).

**Removal and return of goods:** When customers pick up an item from the shelf, two systems register this simultaneously: the camera recognizes the hand movement and visually identifies the product. At the same time, the shelf sensor measures the weight loss at that exact location and confirms that an item has been removed. AI combines both pieces of information – what was taken and by whom – and adds the product to the person's digital shopping cart. If the customer puts an item back, the same thing happens in reverse, and the shopping cart is corrected accordingly (Kausch, 2024). It is important that the system tracks each person's actions individually, even if several people are shopping at the same time. Hundreds of cameras are therefore installed in a cashierless store to cover every angle (Reuter, 2024). This all-round coverage is necessary to rule out any confusion, but it also shapes the store layout: stores are designed with long, straight aisles and few blind spots so that the cameras have a clear view. Here, technology trumps atmosphere in the design (Kausch, 2024).

**Checkout and payment:** The stores in the context of this paper offered different options: Customers with the app can simply scan the app's QR code on their way out, and the stored payment method is automatically charged without any further intervention or payment confirmation on the part of the customer. Alternatively, classical conveyer belts with staff or self-checkout systems can be used. In the latter case the system recognizes the person and automatically provides the items that have been scanned, i.e., they do not have to be taken out of the bag and scanned again. In both cases payment must be made actively by card or smartphone before the customer can leave the store. The hybrid checkout systems allow flexible adaptation to different user preferences, also to address reservations about the new system (Schipkowski, 2024).

When the person leaves the store, their tracking skeleton is deleted or stored pseudonymously for a limited period of time, for example for AI training purposes or for error analysis (Gärtner, 2024; Reuter, 2024). According to the retailer, the raw video data remains available locally on the systems for only a few hours and is then replaced by abstracted data sets, which can be stored in the cloud for up to several days (Reuter, 2024).

## Data Protection

At first glance, the skeleton-based method used in cashierless stores appears to offer advantages from a data protection perspective: it does not require facial recognition and still allows goods to be reliably assigned to anonymized movement profiles. According to the retailer, this complies with the principle of "privacy by design", as no directly identifiable characteristics are recorded, but it does enable a person to be tracked in the supermarket. Data processing can take place locally or in the cloud, whereby temporary storage is often sufficient to complete the checkout process correctly

(REWE, 2023; Reuter, 2024). Accordingly, skeleton-based gait recognition is often presented as a privacy friendly alternative to facial recognition. This creates the impression of anonymous data collection, although in reality highly sensitive biometric profiles are being created. As (Teepe et al., 2022) emphasize, it is precisely this seemingly unobtrusive form of recognition that poses significant risks to privacy.

**Collected data:** As part of the cashierless shopping process, a wide range of sensitive data is processed, mapping the entire movement and interaction history of customers. The collection of movement data in the form of a schematic skeleton representation of the human body plays a central role in this process. In its privacy policy, the retailer explicitly describes "video recording in the store: schematic representation of your bone structure" as the basis for customer recognition (REWE, 2023). In addition to this movement data, interaction data is also collected. The system records exactly when a product is taken from the shelf or put back (REWE, 2023). This information is crucial for the automatic creation of the digital shopping cart and is intended to ensure that only items that have actually been selected are billed.

**Data storage:** According to the retailer, the collected data is not stored locally on a permanent basis, but is processed in a multi-stage process and only stored temporarily (REWE, 2023; Reuter, 2024). First, pre-processing takes place directly on-site using edge computing: the movement and interaction data collected by cameras, sensors, and other devices is analysed immediately on local edge devices. This local processing enables fast response times and reduces the need to transfer large amounts of data to central systems immediately. The relevant information is then transmitted to cloud-based systems for further analysis and billing. The cloud serves as a central instance for aggregating data, managing digital shopping carts, and processing payments.

In this context, it is important to consider how long and in what form image and sensor data is stored. According to official retailer privacy notices, raw video recordings are stored on local devices for up to six hours, after which they are blurred or pseudonymized, and the data is reused in processed form in the cloud. The data is stored in the cloud for a maximum of ten days, in some cases on servers outside the European Union (REWE, 2023). The latter is particularly sensitive in terms of data protection law. As soon as personal data is transferred to a third party country, additional legal precautions are required. Retailer and manufacturer state that they use EU standard contractual clauses, among other things (Trigo Vision, 2022). The blurring and pseudonymization of raw data are considered key protective measures in line with the "privacy by design" approach. According to the retailer this means that no directly identifying personal data is stored (Reuter, 2024). Nevertheless, it should be noted that the recorded movement profiles can be clearly assigned to individual persons, at least internally, which remains problematic in terms of data protection law, especially if the processing takes place on servers outside the EU (Data Protection Conference 2020). Despite technical measures such as pseudonymization and the avoidance of classic biometric methods such as facial recognition, the relevance of data protection law remains high: movement profiles can be used to (re)identify individuals based on their individual gait. Such "soft" biometric features are also subject to the provisions of the GDPR if they are used to identify natural persons (GDPR 2016, Art. 4 No. 14; Teepe et al., 2022).

### IT Security

A key risk of biometric surveillance systems is the high sensitivity of the stored biometric characteristics. According to recital 51 of the GDPR, biometric data is particularly sensitive, as its processing may pose significant risks to fundamental rights and freedoms (GDPR, 2016). If a biometric feature is compromised, the data subject cannot simply reset it, i.e., the compromise is permanent. This makes stolen biometric data sets particularly valuable and usable in the long term for attackers (SOCRadar, 2024).

The systems in cashierless stores are not immune to IT security risks. If this data falls into the wrong hands, for example through a compromised cloud infrastructure or an unsecured edge device, there is also a risk of re-identification, profile abuse, or manipulation of usage processes, especially if the data sets are linked to external sources.

## EMPIRICAL RESEARCH: FIELD STUDY, CUSTOMER SURVEY, AND EXPERT INTERVIEW

In addition to the technological considerations, an empirical study was conducted to examine, confirm, and expand on the opportunities, risks, and challenges discussed. This helps to place the previous statements in a realistic context.

### Observations During a Field Study

Two cashierless stores were visited and tested. This self-testing, supported by qualitative observation, provided insights into practical processes, potential weaknesses from the customer's perspective, and differences between the retailer's presentation and the actual user experience. Note that the findings are based on individual impressions gained through self-observation and cannot be generalized.

In both cases – with and without a special app – access to the store was possible without a QR code. The barrier at the entrance opened automatically, regardless of whether the optional active authentication via the app was used. When using the app, additional guidance on the shopping process was provided via the app. Without the app, however, there was no structured introduction on site; necessary information had to be obtained independently, for example, by asking staff.

Although all customers – regardless of app use – entered the store via the same barrier, this transition was perceived differently in the observation setting. The person shopping with the app subjectively experienced the barrier as the starting point of digital tracking, presumably because app usage was associated with the conscious expectation that the purchase would be automatically recorded. The person without the app, on the other hand, perceived the entrance more neutrally, as no technical activation process was visible from their perspective.

Numerous cameras were visible in both stores, mostly built into the ceiling structure. Differences were apparent in their density and arrangement. Additional technology, such as sensors under the shelves, was barely visible and was not explained in detail.

Regardless of the usage scenario, there was no active explanation of the camera technology on site. In one store, a mobile display with the notice "No facial recognition" was placed in the entrance area, while for the other store a corresponding notice was permanently installed on the exterior facade. Both notices remained vague and did not provide any concrete information about how the system actually works. Overall, the impression was that the technical infrastructure was omnipresent but not communicated transparently, which led to uncertainty and room for interpretation on the part of observers.

When checking out there were minor errors in the billing of goods, which indicates that individual product-related actions were not precisely allocated to persons. This could be due to several people passing items between each other (e.g., family members) or carrying items together, a realistic behaviour that can apparently lead to incorrect bookings in practice.

While the app user could simply leave the store after shopping without actively paying, the self-service customer had to use a stationary card terminal. When using the app, the digital receipt was delivered by email with a considerable delay in some cases (over 15 minutes). Active control or immediate verification of the billed products was not possible. This led to a feeling of lack of transparency. The checkout was convenient, but not transparent, a critical combination, especially when incorrect bills cannot be corrected immediately.

Communication on data protection was formally present in both scenarios, but not very accessible. In both stores, small-print data protection information in DIN A4 format was displayed in the shop window. It was visible from the outside, but easy to overlook and challenging in terms of content.

### Customer Survey

A standardized questionnaire was filled in by 33 random customers, resulting in an exploratory survey with no claim to representativeness. The assessments of the technical functioning of the cashierless store reveal a fragmented and sometimes flawed understanding. The most common assumption was that cameras recognize what is taken from the shelf (17 out of 33 people) and sensors in the shelves detect whether products have been removed or put back (16 mentions).

Eight people stated that cameras and AI analyse how they move around the store. This indicates that at least some of the respondents implicitly understood or at least noticed a form of motion capture. Two people mistakenly assumed that their faces were being scanned, a fallacy that may be encouraged by the physical presence of the cameras and unclear visual communication. Ten participants even assumed that only the goods were being recorded, not themselves. Three people stated that they did not know how the system works.

The retailer's data protection notices were hardly noticed at all. Only four of the 33 respondents stated that they had even noticed the small print notice in the shop window. Only one of these four also read the complete text. Another participant at least skimmed it, while two did not. The overwhelming majority (N=29) did not pay any attention to it. Reasons given for the lack of engagement included lack of time and a feeling of being sufficiently informed by prior knowledge or visible notices. This behaviour points to a pattern of cognitive load reduction. The mere presence of data protection notices is apparently perceived as a substitute for genuine engagement.

The note "No facial recognition" was noticed by 16 participants. Eight of them felt sufficiently reassured by this note and deliberately refrained from seeking further information on data processing. The remaining eight nevertheless expressed further interest in the technical processes. Overall, the effect of the note remains ambivalent. On the one hand, it creates short-term trust, but on the other hand, it seems to reduce the motivation for in-depth discussion.

When asked about the possible purposes for which the retailer uses collected movement data, participants could select several options. The most common assumptions were: improving the shopping experience (16), optimizing the product range (12), improving navigation/store layout (10), security in the store (6), advertising purposes (4), and other (3). The data shows that many respondents assume that the data will be used in a customer-centred and service-oriented manner. The possibility that advertising or potential security monitoring could also play a role is less commonly assumed.

20 out of 27 respondents expressed surprise when they were confronted with the fact that their movements are also recorded when they do not pay with the app – as an accompanying person or when paying at a traditional checkout. Opinions regarding the recordings were divided: eight people found this problematic, twelve were neutral, and seven found it unproblematic.

Overall, the apparent lack of transparency jeopardizes informed consent and undermines central principles of data protection-compliant technology design.

## Expert Interview

As last empirical study, a guided interview was conducted with an editor of a digital civil liberties publication and renowned expert on digital surveillance, who is referred to here only anonymously.

**Legal and regulatory aspects:** A central topic of the interview was the legal classification of cashierless store systems. The expert points out numerous gaps and uncertainties of interpretation within the GDPR. He emphasizes that although the legal framework offers basic protection, he criticizes its vagueness and unclear wording. This gives companies leeway to evade effective regulation. He is particularly critical of the fact that biometric procedures are not identified as such by the retailer. Semantic reinterpretations are used to circumvent stricter data protection rules. Institutional weaknesses in enforcement are also addressed, such as inadequate control by supervisory authorities or potential government access to privately collected movement data. Private and state surveillance can hardly be separated today. He also warns of the risks of outsourcing sensitive data to international cloud providers, for example through contracts with system manufacturers outside the European Union.

**Technical and data-related risks:** The expert describes the cashierless store system as a technologically fragile system that is still in the experimental stage. He particularly questions the seamless recording of physical characteristics such as movement and clothing, even without the use of an app. Biometric recognition (re-identification) is therefore possible even without classic facial recognition. He is particularly critical of the secondary use of the collected data for training purposes or internal system optimizations. He cites further risks such as possible manipulation due to technical malfunctions and insufficient protection against data misuse and hacking.

**User perspective and perception:** The expert points to a significant information asymmetry between retailers and consumers. He says that the information provided is insufficient and that even when specific questions are asked, many technical processes remain unclear. He also criticizes a deliberately misleading communication policy. Although it is publicly emphasized, and even used in reassuring advertising, that facial recognition is not used, the biometric method of skeleton tracking that is used is not named as such. This makes it difficult to clearly classify the system in terms of data protection law. The practice of providing information in accordance with the GDPR is also hampered by structural opacity. Responsibility for technical errors is not clearly defined, which can create uncertainty among users.

## CONCLUSION

The analysis of cashierless store systems makes it clear that their evaluation must not be limited to technical efficiency or economic potential. Rather, there is a complex interplay between technological feasibility, legal requirements, and social acceptance.

The theoretical foundations of biometric methods, AI-based video analysis, and data protection were substantiated by empirical findings from field observations, a customer survey, and an expert interviews. This revealed not only functional aspects, but also differences between technical implementation and perception. In particular the survey showed that most users are hardly aware of these risks. The technical infrastructure is taken for granted, coupled with the confidence that the provider will ensure adequate security.

The data protection practices examined in the field study reveal a clear discrepancy between formal communication and actual practice. Customer re-identification is possible through the collection of skeleton-based movement profiles and the assignment of temporary IDs. When the stored movement patterns are linked to purchasing behaviour, transactions, or other metadata, comprehensive digital profiles are created. This practice is problematic from a data protection perspective. Processing of such sensitive data requires either the explicit consent of the data subjects or a clearly defined legal basis.

## REFERENCES

Bahr, Ines (2022): Kassenloser Supermarkt: der neue Trend des stationären Handels. Capterra. Online: https://www.capterra.com.de/blog/2572/kassenloser-supermarkt [Last accessed: May 19, 2025].

Data Protection Conference - Datenschutzkonferenz (2020): Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen. Hrsg.: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg.

EHI Retail Institute GmbH (2023): Re-start des stationären Handels. Online: https://www.ehi.org/presse/re-start-des-stationaeren-handels/ [Last Accessed: July 2, 2025]

EHI Retail Institute & KPMG (2024): Self-Checkout: Studie zeigt große Akzeptanz bei jungen Kunden. Online: https://www.retail-news.de/kpmg-ehi-studie-self-checkout-deutschland/ [Last accessed: June 30, 2025]

Franken, Roxane (2021): Der kassenlose Supermarkt und der Datenschutz. Datenschutz Notizen. Online: https://www.datenschutz-notizen.de/der-kassenlose-supermarkt-und-der-datenschutz-2132596/ [Last accessed: July 1, 2025].

Gärtner, Josephine (2024): Kassenlose Supermärkte – Datenschutz beim Einkaufen, Dr. Datenschutz. Online: https://www.dr-datenschutz.de/kassenlose-supermaerkte-datenschutz-beim-einkaufen/ [Last accessed: May 19, 2025].

GDPR - Datenschutz-Grundverordnung (DSGVO) (2016): Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung). Online: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679 [Last accessed: July 7, 2025].

German Trade Assoziation- Handelsverband Deutschland (2024): Tag der Arbeit: Einzelhandel hält Beschäftigung stabil, warnt aber vor Gefahr von Fachkräftemangel und zu hohen Sozialversicherungsbeiträgen. Online: https://einzelhandel.de/presse/aktuellemeldungen/14797-tag-der-arbeit-einzelhandel-haelt-beschaeftigung-stabil-warnt-aber-vor-gefahr-von-fachkraeftemangel-und-zu-hohen-sozialversicherungsbeitraegen [Last accessed: Mai 19, 2025].

Kausch, Martina (2024): Store-Check spezial Rewe Hamburg Hoheluftchaussee: Unter den Augen der KI. RUNDSCHAU für den Lebensmittelhandel. Online: https://www.rundschau.de/service/artikel/store-check-spezial-rewe-hamburg-hoheluftchaussee-unter-den-augen-der-ki [Last accessed: July 10, 2025]

MWIKE - Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen (2024): Zukunft des Handels: Einkaufsverhalten und alternative Einkaufsmöglichkeiten in NRW. Düsseldorf: MWIKE NRW. Online: https://www.wirtschaft.nrw/system/files/media/document/file/hsk_studie-wimi-nrw161224.pdf [Last accessed June 30, 2025]

Parashar, Anubha; Parashar, Apoorva; Abate, Andrea F.; Shekhawat, Rajveer Singh; Rida, Imad (2023): Real-time Gait Biometrics for Surveillance Applications: A Review. In: Image and Vision Computing, 138(1), Article 104784. Online: https://www.sciencedirect.com/science/article/pii/S0262885623001580?via%3Dihub [Last accessed: June 30, 2025].

Pettigrew, Mark. (2025): Optimizing space and assortment for hybrid shopping. RELEX Solutions. Online: https://www.relexsolutions.com/resources/hybrid-shopping/ [Last Accessed: May 19, 2025].

Reuter, Markus (2024): Panoptischer Rewe-Supermarkt: Einkauf mit Skelettkontrolle. netzpolitik.org. Online: https://netzpolitik.org/2024/panoptischer-rewe-supermarkt-einkauf-mit-skelettkontrolle/ [Last accessed March 25, 2025].

REWE Group (2022): Offizieller Start in Berlin: REWE Pick&Go bringt hybriden Supermarkt mit kassenloser Bezahlmöglichkeit für alle Kundinnen und Kunden in die Hauptstadt. Online: https://www.rewe-group.com/de/presse-und-medien/newsroom/pressemitteilungen/offizieller-start-in-berlin-rewe-pickgo-bringt-hybriden-supermarkt-mit-kassenloser-bezahlmoeglichkeit-fuer-alle-kundinnen-und-kunden-in-die-hauptstadt/ [Last accessed: July 1, 2025].

REWE Group (2023): Auf Erfolgskurs mit neuer Technologie: Drei weitere REWE Pick&Go Märkte in Düsseldorf und Hamburg. Online: https://www.rewe-group.com/de/presse-und-medien/newsroom/pressemitteilungen/auf-erfolgskurs-mit-neuer-technologie-drei-weitere-rewe-pickgo-maerkte-in-duesseldorf-und-hamburg/ [Last accessed: June 30, 2025].

Schipkowski Katharina (2024): Abgescannt – Überwachtes Einkaufen in Hamburg. Taz – die tageszeitung. Online: https://taz.de/Ueberwachtes-Einkaufen-in-Hamburg/!6045235/ [Last accessed: July 10, 2025].

Sluiter, Amelie (2022): Kassenloses Einkaufen und der Datenschutz. WS-Datenschutz. Online: https://webersohnundscholtz.de/kassenloses-einkaufen-und-der-datenschutz/ [Last accessed: May 19, 2025].

SOCRadar (2024): Biometric Security Risks: Beyond Fingerprints and Facial Recognition. Online: https://socradar.io/biometric-security-risks-beyond-fingerprints-and-facial-recognition/ [Last accessed: July 16, 2025].

Teepe Torben, Gilg Johannes, Herzog Fabian, Hörmann Stefan, Rigoll Gerhard (2022): Towards a Deeper Understanding of Skeleton-Based Gait Recognition. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), pp. 1569–1577.

Trigo Vision (2022): Privacy Policy. Online: https://www.trigoretail.com/privacy-policy/ [Last accessed: April 14, 2025].

Trigo Vision (2024): Unveiling Retail's Invisible Crisis: How Trigo Makes Shrink Visible. Online: https://www.trigoretail.com/how-trigo-makes-shrink-visible/ [Last accessed: April 14, 2025].