The body as permanent digital identity? Societal and ethical implications of biometrics as mainstream technology

Stefan Strauß
Austrian Academy of Sciences

Corresponding author
Stefan Strauß
Institute of Technology Assessment,
Austrian Academy of Sciences
Bäckerstraße 13, 1010,
Vienna, Austria
✉ sstrauss@oeaw.ac.at

Submitted: May 24, 2022
Accepted: May 8, 2023

Abstract
There is a global trend to expand biometric technology usage: digital identification practices increasingly gather peculiar features of the human body – in the security domain as well as in the consumer sector and everyday-technologies. This indicates a wider shift in the role of biometrics for digital identification entailing a significant further expansion of identifiability. Applying biometrics is frequently justified with security improvements. However, it also bears various security risks and individuals cannot simply opt-out from their bodies or change their bodily characteristics. On the longer run, human bodies may become partially reduced to enduring machine-readable, informational patterns as physical and digital environments conflate. Biometrics is thus a very powerful and threatful technology increasingly affecting how humans relate to technology, substantially challenging human rights. The paper argues that the far-reaching consequences of this development are yet underestimated and require broader societal debates and regulatory measures to reduce the corresponding risks, in particular as: 1) biometric information is bound to human bodies and thus irreversible, making individuals more vulnerable to misuse; 2) the shift from a security towards a mainstream technology fosters habituation effects and incremental compulsion to provide biometric features; 3) the extensive use of biometric systems facilitates misuse, reinforces surveillance tendencies, security, data protection and privacy issues; 4) biometrics used as automated control technology seriously strain human rights as it reinforces risks of discrimination, increasingly affecting bodily integrity and human dignity.

Keywords
identification practices; digital transformation; privacy; security; dignity; human rights.

1. Introduction

Biometrics has a long history and its usage as identification practice for security purposes in Europe dates back to the 19th century (Lyon 2008; Maguire 2009; Jain 2016). Beginning in the 1990s, it became a tool of global security governance, latest in the aftermath of the 9/11 terrorist attacks. Many scholars in security and surveillance studies extensively analyzed this role and its societal con-

sequences (cf. Schneier 1999; Lyon 2003; Bennett and Lyon 2008; Ball et al. 2012). In private sector, diffusion increased as well, though, mainly used as specific security technology in limited contexts, e.g., for law enforcement, border control, or in identity (ID) systems for access control in public and private organizations. For several years now, this role as security technology has been altering within the accelerating digital transformation of society. A significant expansion of biometrics as digital identification practice is observable in various domains. In parallel to its relevance for security governance, also a growing number of commercial applications and "everyday-technologies" employs biometrics. Bodily features like fingerprints or facial images are gathered in many contexts and enormous amounts of biometric information flow into various digital platforms. This often happens either *en-passant*, embedded into typical user verification procedures (e.g., logins); or covertly and without direct user involvement (e.g., through facial recognition systems).

If this development proceeds, biometrics becomes a widespread sociotechnical practice deeply altering digital identification, and how human bodies relate to technology. On the longer run, biometrics showcases the incremental conflation between physical and digital representations of ourselves. This involves some important questions, such as: what are the peculiarities of biometrics as digital identification practice and how does this relate to notions of embodiment? What are main drivers of the global increase in biometrics, and what are the societal and ethical effects of the entrenchment of biometric systems in a broad range of applications? A fully comprehensive analysis of these questions is beyond the scope of this paper but it contributes to this discussion by outlining how this development emerged and providing a critical analytical review of the wider societal and ethical implications of a general expansion of biometrics as digital identification practice in everyday-life. Based on this, the paper argues that the expansion of biometrics entails wider sociotechnical shifts which reinforce identifiability of individuals. Human bodies are increasingly exposed to technologies, secretly measuring and transforming their digital representations into enduring machine-readable code. This has substantial consequences on privacy, security and human dignity. In public discourse as well among policy makers, this development is yet underestimated and requires a broader societal debate and regulatory measures to reduce the corresponding risks.

The paper is structured as follows: the next section presents and discusses analytical perspectives to explore the peculiar role of biometrics as digital identification practice and how it affects the notion of embodiment through technology. Based on this, the empirical sections then first present an analytical review of main political and economic drivers behind the expansion of biometrics and its shift towards commercial applications as mainstream technology. This is followed by an analysis of societal and ethical implications of the extended use of biometrics as digital identification practice. The final section presents a short summary and concluding remarks.

2. Unfolding analytical perspectives

2.1 The peculiar role of biometrics as digital identification practice

Biometrics can be analyzed from various disciplinary angles, e.g., biology and anthropology (Maguire 2009), criminology, sociology and political science (Amoore 2011; Bennett and

Lyon 2008; Mordini and Tzovaras 2012), body, gender and identity studies (Magnet 2011; Smith 2016), computer science, privacy and information security (Schneier 1999; Clarke 2001/2002; Jain 2016; Dong et al. 2022), surveillance studies (Lyon 2003; Ball et al. 2012) etc. From an STS perspective, biometrics is understood as socially constructed technology with mutual processes of co-shaping, i.e., societal practices affect technology design, its political and economic usage patterns and vice versa (cf. Bijker et al. 1989; Feenberg 2002). Correspondingly, the analytical focus here is on biometrics as digital identification practice and the interplay of its sociotechnical and its sociopolitical dimensions. To grasp the wider societal and ethical implications of biometrics requires some basic knowledge on its technical role first.

From a technical angle, biometrics is the processing of digital information of bodily features to authenticate or identify a particular person in specific contexts. Biometric features are inevitably coupled to the human body and thus considered as suitable factors for these purposes (Bennett and Lyon 2008; Maguire 2009; Jain et al. 2016). Identification is "the processing of information related or referring to the identity of a particular individual" (Strauß 2019, 36). Hence, information about a person or more precisely – personally identifiable information (PII) obviously is a necessary condition for identification. There are four basic dimensions of PII (i.e., substantial, spatio-temporal, relational and interactional PII) that together constitute the identifiability of an individual person (ibid, 244). In this regard, biometric features are at the core of substantial PII: they represent specific characteristics substantially bound to a person's body. Biometrics transforms this information (e.g., of a physical fingerprint or a facial image) into digital representations thereof. Besides the widespread use of fingerprints or facial images, various systems also gather other bodily features like informational patterns of the iris, voice or even vein patterns, or additional sensor data like skin temperature, pressure etc. (Jain 2016; Schaber et al. 2020). Due to its integration into other digital technologies (e.g., via sensors in smartphones, laptops or smart CCTV etc.), biometrics are often combined with technically generated identifiable information (TII), like, e.g., device- and application specific IDs, sensor IDs, digital hash-values, geo-location/movements, time stamps, relational and interactional information and many other forms of meta data (Strauß 2019, 245).

The peculiarities of biometrics also affect the sociopolitical role of the human body and how it is represented and used by technology. Due to the inherent identifiable nature of biometric features, they always convey the possibility to identification. Hence, even though biometric features serve authentication, identification is hardly avoidable – even if unintended. In the notion of the body as a "walking sensor platform" Smith (2016, 110) conceptualizes this issue as "disembodied exhaust" which "refers to the data trails that, as affective transfers, are either voluntarily or involuntarily emitted from the body as it interfaces with networked sensor technologies". In contrast to other forms of identity information used as credentials, biometric features are not changeable. Once in use as credentials, they are a persistent representation of a person's identity based on characteristics of her body. The digital processing of biometric characteristics thus has consequences for their persistence and durability and thus also for the identifiability of individual persons and how they are embodied by and through technology.

2.2 Humans as tool-beings? How biometrics affects embodiment

The increasing use of biometrics is a showcase to the questions how our bodies become digitized and how digital technology alters embodiment. Various studies discuss effects of technology on embodiment concerning self-presentation, e.g., in the context of social networks or virtual environments (Kruzan and Won 2019). Few studies examine how digital technology and biometrics tend to reduce embodiment to digital representations of human bodies (Farr et al. 2012). Titchkosky (2007, 13) broadly defines embodiment as "all the [...]ways that we (self and other) accomplish relations to being in possession of the bodies that we are". Based on this, Melonocon (2013, 71) highlights the role of technology for embodiment and in reference to Heidegger, argues that due to technology usage, humans are "tool-beings that use a variety of equipment, or technology". In other words: technology temporarily becomes a functional part of the body through interaction. This is basically given for any form of human-computer interaction but not necessarily including identification as in the case of biometrics.

Biometric technology is thus a specific case with additional effects altering the classical notion of embodiment: it generates a digital representation of features of the human body (e.g., fingerprints or facial characteristics) which then serves as identification tool. On a general level, a digital artifact based on reductionistic models of bodily features emerges inevitably referring to an individuals' identity. In this regard, the notion of "humans as tool-beings" gets a different meaning: not just technology is a tool for humans, but features of the human body serve as tools for biometric technology in various contexts. Correspondingly, scholars in surveillance studies describe biometrics and the gathering of bodily information through digital technology as process where human bodies are converted into "data derivatives" (Amoore 2011) or "objects of information" (French and Smith 2016; Smith 2016). There is thus also a nexus of embodiment and surveillance. Through biometrics, the body as object of information becomes metaphorically liquified (ibid.), as Lyon describes with the concept of: "liquid surveillance" that:

> captures the reduction of the body to data and the creation of life-chances and choices hang more significantly than our real lives and the stories we tell about them. (Lyon 2010, 325; cited from Smith 2016)

Basically, surveillance and control practices always relate to identification practices (Clarke 2001; 2002; Lyon 2008; Ball et al. 2012; Smith 2016; Strauß 2019). Biometric technology, which is basically driven by the notion that bodily features are a dependable source for identification, tightens this relation. It combines personal with technical identification and transforms bodily information into machine-readable code. This "ontology of the body as a reliable organism for identification and measurement has helped turn bodies into focal points for practices of monitoring and control" (French and Smith 2016, 8). Biometrics is thus a very powerful, transformative technology fostering the incremental conflation between physical and digital representations of human identities over their bodies.

In a figurative sense, biometrics dematerializes bodily features and transforms them into digital matter. Apparently, this is not a direct transformation as the body obviously remains matter. But bodily information becomes virtualized and a virtual entity of ourselves emerges.

This virtual entity is then exposed to further processing, stimulating a further expansion of identifiable information and thus of identifiability. From a metaphysical perspective, referring to Karen Barad's theory of agential realism (Barad 2007), biometrics is an example of an interactional process or "intra-action" that creates informational objects of the human body which enable the possibility of alternative usage. On the longer run, these alternative usage forms can pave the way for further transformations even involving transhumanism as biometrics is closely related to AI. But also leaving this metaphysical approach aside, the transformative capacity of biometrics has far-reaching consequences for the role and function of bodily features in society.

3. Empirical analysis

3.1 From security to commercialization: biometrics as mainstream technology?

The use of biometrics for identification as administrative practice has a relatively long history. Early biometric ID systems in Europe date back to the 19th century in France and were also used by the colonial powers, e.g., by the British administration in India (Maguire 2009). Partially, this historical context affected the creation of systems like Aadhaar in India, which today is the largest governmental biometric ID database system with over 1.2 billion entries (Rao and Nair 2019). In national contexts, biometrics are used for many years for law enforcement and security governance. In the aftermath of the 9/11 terrorist attacks, this increased significantly on a global scale. Its use for identification as part of global security governance began with the integration of biometric features into passports and other forms of governmental IDs (Bennett and Lyon 2008; Maguire 2009; Magnet 2011). Since 2005, biometric data and radio-frequency identification (RFID) became a standard feature in newly rolled-out passports[1] (Bennett and Lyon 2008). Nevertheless, biometrics mainly served as specific technology in limited contexts in the security domain, e.g., for law enforcement, border control or access control systems in public and private organizations.

For several years, though, a significant expansion of biometrics proceeds, including a variety of commercial applications ranging from smartphone apps, e-banking, payment services, smart locks, digitized vehicles up to internet of things (IoT) applications. Gathering biometric information thus is about to become a common practice embedded into various everyday-services. This often happens either as additional process in a typical user verification procedure (e.g., user logins), where biometrics like fingerprints or facial image are used for multi-factor authentication; or covertly and without direct user involvement (e.g., through facial recognition). Also operating systems on PCs and laptops increasingly suggest to use biometrics as user credentials. All these developments lead to an incremental increase in the gathering of bodily features in various contexts.

This trend continues and over the years, there has been a shift where biometrics turned from being a security technology in a limited number of domains towards a convenience technology being broadly applied in the consumer sector. In many Asian countries, this trend started earlier and over the last years, applications significantly increase also in the US and Europe, where, e.g., global payment companies like Mastercard and Visa started about 2013

with payments via biometrics like "pay-by-selfie" (Sayer 2013; Leyden 2016). This development towards biometrics as mainstream application is not just pushed by the tech-industry, but also by policy makers in Europe: The EU Commission frames biometrics as key enabler for future digital services to stimulate digital markets (Bonneau et al. 2018). Correspondingly, various regulations, e.g., the eIDAS Directive[2] of 2016 foresee an interoperable, cross-border digital identification framework for public and private services. Further regulations refer to this framework, like the EU payment services Directives[3] to stimulate the use of digital IDs in online markets. Recent plans to amend the eIDAS Directive[4] aim at further broadening usage of the digital ID framework by, e.g., introducing digital wallets for EU citizens. Since 2019, e.g., the payment services Directive explicitly forces service providers to multi-factor authentication to improve security in online services. This means that the identity of a person needs to be verified based on at least two security factors. These are either *knowledge* (i.e., a password or PIN), *possession* (i.e., a token like a smart card), or *inherence*, i.e., a metric intrinsically linked to an individual. The latter basically means biometric features like fingerprints, facial image, voice pattern or other bodily characteristics. Biometrics is not mandatory, though, recommended. Therefore, most providers integrated biometrics into their applications like, e.g., in some smartphone-apps for e-banking or mobile payment. This technology push is one reason for its growing importance across Europe. The ongoing global trend towards a commercialization of biometrics affects a broad range of public and private services. In combination with plans of the technology-alliance FIDO including big tech-companies (e.g., Microsoft, Apple, Google) to replace password-based user logins with biometrics (FIDO 2022), a significant technology-boost in the next few years can be expected.

This makes biometric data even more attractive for additional usage like profiling based on so-called identity graphs. For several years, global tech-companies like Facebook/Meta, Google/Alphabet, Amazon or database companies like Oracle and others build ID graphs to dynamically map and analyze user data also across different technologies. These ID graphs stimulate new markets with digital identities. Identity information is being gathered "across all devices, screens and channels" in order to create comprehensive ID models of consumers "including what people say, what they do and what they buy" (Oracle 2015; Strauß 2019, 138). With the further commercialization of biometrics, these ID graphs also include bodily features (Christl 2017). Biometrics thus also serves global data markets. This global expansion of the gathering of biometric information in commercial applications relates to Zuboff's notion of "surveillance capitalism" addressing the increasing tendency of processing data on human individuals and their behavior for commercial business models (Zuboff 2019, 8ff.). In parallel, policy makers also extent the processing of biometric data for law enforcement and security authorities. In Europe, the amendment of the Prüm framework[5] ("next generation Prüm") inter alia foresees more use of biometrics and data exchange for security authorities. These plans include the implementation of a cross-broader facial recognition system (EP 2020; EDRi 2021). Altogether, these developments are driven by an ongoing trend of securitization and economization of digital identification (Strauß 2019, 134). This is a further indicator for the conflation between political and economic variants of "surveillant assemblages" (Haggerty and Ericson 2000). This conflation and the broader use of biometrics entails serious societal and ethical risks as discussed in the next section.

3.2 Societal and ethical implications

Essentially, the broad use of biometrics leads to increasing identifiability of individuals. This raises many societal and ethical issues with far-reaching effects on human rights and democracy, which result from a mix of social, political, economic and technological factors:

3.2.1 Irreversibility and vulnerability of biometric information

A crucial peculiarity of biometric features is its strong and inevitable linkage to the body of a particular person. This can facilitate to enforce identification, as biometrics always conveys information about the identity of the person. The main argument justifying the use of biometric technology is to improve both: security and convenience of identification and authentication procedures. However, this argument is only partially valid. Potential security gains are achievable in cases where hard identification is necessary and where the application environment is securely protected from misuse. In theory, biometrics require the physical presence of the person concerned which should decrease the risk of security breaches. This is assumed to be a security benefit compared to common credentials. Biometric features are thus attractive as factor of inherence for multi-factor authentication. However, in fact, biometrics only make sense in clearly defined, secure environments where abuse is very unlikely and systems are decoupled from external access (Schneier 1999; Clarke 2001; 2002; Schaber et al. 2020). Particularly, because the irreversibility of biometric information affects the severity of various risks: when common user credentials (e.g., username and password) are misused, an effective method to limit further damage is revocation and change of credentials. In contrast to less binding forms of identifiable information, bodily characteristics, though, are not changeable and cannot be easily revoked. In other words: a person may change its username, real name or any other identifiers, but she cannot opt-out from her body by changing her face or fingerprints. The general irreversibility of biometric features thus also affects its vulnerability, may facilitate abuse and limit options to take effective action to prevent it. In practice, numerous variants of attacks on biometric systems exist, even without requiring physical presence (Adler and Schuckers 2009; Hadid et al. 2015; Ramachandra and Busch 2017; Dong et al. 2020). Security researchers demonstrated, e.g., to easily gather fingerprints from a glass or other surfaces with adhesive strips to create synthetic fingerprints; digital images can circumvent facial recognition and common digital cameras are sufficient to trick even more complex biometric sensors like iris-scans (Arthur 2013; Foltýn 2019; Schaber et al. 2020). Moreover, recent studies show that inverse biometrics, i.e., the abusive reconstruction of biometric templates, is possible: biometric templates (the digital encoding of biometric features) are used to avoid direct processing of biometric information (e.g., fingerprint) and were assumed to be widely protected from reverse engineering and abuse. However, several studies demonstrate that they are not as secure as assumed (Gomez-Barrero and Galbally 2020). This increases the vulnerability of biometric systems and risks of privacy breaches, unintended secondary use or other forms of misuse. Extended usage of biometrics will likely aggravate these problems.

3.2.2 Habituation effects and incremental compulsion to provide biometric information for identification

As a consequence of biometrics as mainstream technology, individuals become increasingly confronted with and thus used to providing bodily features in everyday-life. Already today, various smartphone apps gather biometric features such as the Chinese social media app Tiktok collecting personal faceprints and voiceprints (Perez 2021). Similar is the case for other social media services which hold enormous amounts of facial images of their users worldwide (e.g., Facebook/Meta or its subservices Whatsapp and Instagram; see Field 2021). One may argue that users are not obliged to use biometrics. However, its expansion facilitates function and mission creep: i.e., extended use of the technology in various application contexts beyond its original purpose (Lyon 2003; Ball et al. 2012), accompanied by a gradual decrease in alternatives without biometrics. Individuals being uncomfortable with providing their bodily features may encounter difficulties in avoiding biometrics. This is already observable, e.g., in banking apps mostly suggesting to provide biometric features for authentication. Also other domains like the mobility sector include biometrics: some cars already use fingerprints instead of keys which is part of a general trend in the automotive industry to foster biometrics like fingerprint scans, facial recognition and iris scans (Eisenstein 2018; Burt 2021). Moreover, biometric recognition also functions without direct user involvement. The global trend towards facial recognition is a showcase for this: these systems can covertly identify individuals from a distance. Their functionality also refers to habituation effects: many people provide and share their facial images via smartphones and social media. As this data is mostly not protected from external access, it can be harvested and, e.g., used to train facial recognition algorithms. For instance by Facebook, having introduced facial recognition in 2010 (Strauß 2019, 172) or biometric search engines like "Clearview AI" or "Pimeyes" that harvested millions of facial images from the internet. There is also a growing number of facial recognition apps and smart glasses equipped with biometrics available. Google developed a similar technology already in 2012 but stopped it also due to heavy protest and concerns of privacy and security experts (Eveleth 2018). However, the technology seems to recur. Recently, Clearview AI announced that it develops such a technology for the U.S. Airforce (Brewster 2022).

3.2.3 Additional risks of security breaches, privacy violations and surveillance

The expanding range of "everyday"-applications processing biometric features makes abuse of various kind (e.g., identity theft) even more attractive. Attackers benefit from broad usage of biometrics as misuse pays off: once biometric features are gathered they can be misused in various contexts. The growing amount of security breaches and attacks on biometric systems underlines risks of misuse, e.g.: in 2019, 184,000 datasets of a facial recognition system of US homeland security were stolen and sold in the darknet; also in 2019, security researchers revealed that the database of a large security company providing biometric systems worldwide was unprotected from external web-access. It contained 28 million entries including fingerprints and facial biometrics; in 2020, over 70,000 datasets with fingerprints were stolen from a database of the Brazilian government; Aadhaar, the largest biometric system in In-

dia, containing the highest amount of biometric data worldwide (more than 1 billion) is frequently getting hacked. In 2018, biometric data from Aadhaar were even sold via Whatsapp (Malhotra 2018); and in 2021, media reported about government backed Chinese hackers attacking the system (Tarabay 2021). But not only direct attacks to biometric systems are security threats but also insufficient protection, lacking risk-awareness and careless provision of biometric data. Smartphones become centralized devices for biometric processing and thus are very attractive for misuse of various kind. Particularly social media offer various options to exploit biometric data like facial images.

Secretly gathering biometric features over digital technology is thus relatively simple and misuse is evident as scandals like those around Pimeyes in Europe and Clear View AI in the US highlight: both companies harvested facial images from web sources on a global scale to train their facial recognition systems (Laufer and Meineck 2020; Hill 2020a). These are not single cases: there are, e.g., also several lawsuits for misusing biometric data against Facebook/Meta (EPIC 2018; Paxton 2022). Besides the legal and ethical problems, these practices also highlight a policy vacuum as regards the protection of publicly available information containing biometric features like facial images. German federal state Baden-Würtemberg initiated legal proceedings against Pimeyes[6] and in March 2022, the Italian Privacy Regulator fined Clearview 20 million USD for violating the GDPR (EDPB 2022). These lawsuits are important but a decrease in biometrics is still doubtful. Basically, the GDPR considers the sensitive nature of biometric features and the power of biometrics: it defines biometric data as:

> personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. (Art. 4 GDPR[7])

Given the sensitivity of biometric information, the regulation foresees a higher level of protection for biometric data and prohibits its processing "for the purpose of uniquely identifying natural persons" (Art. 9 GDPR). Hence, theoretically, biometric information is sensitive, requires thorough protection and the use of biometric systems is legally restricted. However, in practice, this is rather ineffective, due to several exceptions and an old problem, i.e., the limits of informed consent (Strauß 2019, 198ff.), individuals mostly lack in effective options to avoid being exposed to biometric identification. As of yet, there is often no real alternative except for explicit non-usage of applications processing biometric information. Moreover, boosted by social media, there are millions of selfies and other facial images available, exposed to misuse of any kind without any effective protection as these and other data scandals show. The above-mentioned lawsuits are rather the tip of the iceberg. With further normalization of biometrics, increasing pressure on individuals to give consent can be expected. Altogether, the broad accessibility of biometric data over digital technologies stimulates their massive collection and increases risks of misuse. This is a further indicator for the invalidity of the argument that biometrics would improve security.

Clarke (2002) early warned of biometrics being among the most dangerous technologies reinforcing mass surveillance. Particularly, as biometric technology is an integral part of "sur-

veillant assemblages" (Haggerty and Ericson 2000) where "assemblages leak into assemblages, with no clear sense of where the body stops and where surveillance systems start, and vice versa" (French and Smith 2016, 10). This assumed leakage from one assemblage to another basically means re-contextualization and secondary use of biometric data in terms of data protection. The broad usage of biometrics can thus indeed lead to a severe reduction of anonymity, privacy and related other fundamental rights like freedom of movement, expression etc. Furthermore, also human dignity is already affected in many respects.

3.2.4 Risks of reinforcing discrimination and incremental reduction of human dignity

The irreversibility of biometric information also reinforces risks of discrimination and affects human dignity. Many scholars have been warning for years about the manifold risks of biometrics to human rights (cf. Schneier 1999; Clarke 2001; 2002; Lyon 2008; Magnet 2011; Ball et al. 2012; Mordini and Tzovaras 2012; French and Smith 2016; Schaber et al. 2020; Gordon et al. 2021). Through biometrics, we are partially becoming reduced to algorithmic codes, entailing the risk of an incremental dehumanization of ourselves, as Clarke (2001) put straight. As of yet, this risk of a dehumanization may sound overstated. However, given the fact that biometric systems increase globally, implying the automated, algorithmic mapping, classification and encoding of information concerning human bodies, this risk may increase significantly. Not least as biometrics is closely linked to automated statistics, machine learning algorithms and AI. Algorithmic systems increasingly use biometric "body codes" to govern, predict and control human behavior. This is evident for many years in authoritarian regimes where biometric technology such as facial recognition serves as tool of discrimination and oppression, e.g., to identify government critics or to identify, categorize and divide citizens in different social groups. For instance, in China, where the technology is used to control citizens and sort out unwanted minorities like Uygur Muslims (Ng 2020); similar in Russia, where the technology serves mass surveillance and the prosecution of opposition members (HRW 2021); or in Iran, where the authoritarian regime plans to use facial recognition to identify women who are not wearing hijabs (Strzyżyńska 2022).

The increasing use of biometrics as political tool of control is not limited to non-democratic regimes but also observable in democratic states. Among others, Magnet (2011, 126) argued that biometrics lead to a revival of outdated biological notions about race and gender. The technological reinforcement of structural discrimination and racism is an evident problem today. Facial recognition is particularly problematic here which, as many cases (also outside the US) demonstrate, frequently leads to false accusations and discrimination. One issue is that biometric systems are often prone to errors. For example: during a soccer game in Wales in 2017, a facial recognition system falsely classified more than 2,000 persons as suspects which corresponds to an error rate of over 90 per cent (Burgess 2018). A further example is a system used in the US city of Detroit which even had a failure rate of 96 per cent as the head of police admitted (Koebler 2020). Failure rates may decrease due to technological progress. However, this does not solve societal and ethical problems as lacking accuracy is only a side issue while the main issue is how the technology is used (Castelvecchi 2020). A serious problem of growing concern are false accusations and structural discrimination: in 2020, Robert

Williams became the first person being discriminated by facial recognition. He had to spend several hours in jail just because he was classified as suspect based on an algorithmic image similarity (Hill 2020b). Williams is not a single case, e.g., also Michael Oliver and Nijeer Parks were arrested because of deficient facial recognition (Hill 2021). A large-scale study in the US revealed that people of darker skin color become up to 100 times more falsely identified by facial recognition than whites (NIST 2019). This underlines the problem of inherent bias in facial recognition and how this kind of technology reinforces institutional racism and other forms of discrimination. These risks aggravate also in Europe due to increasing tendencies to extend the use of biometrics for law enforcement. As aforementioned, the EU commission plans a new Directive to foster automated data exchange for police authorities, including a stronger focus on biometrics, particularly facial recognition. Several civil rights organizations expressed concerns arguing that this paves the way for mass surveillance and the erosion of the presumption of innocence, which is a core principle of democracy. Criticism also includes examples of former misuse and systematic flaws in data protection (EDRi 2022).

As biometrics imply reducing bodily features to digital data, this can also affect bodily integrity and human dignity. These human rights aim to ensure self-determination of humans over their own bodies. According to Art. 1 of the EU Charter of Fundamental Rights (EUCFR): "Human dignity is inviolable. It must be respected and protected." Art. 3 EUCFR determines that: "1. Everyone has the right to respect for his or her physical and mental integrity". However, a significant increase in biometric practices further strains these rights. Even without direct abuse, autonomy and self-determination are affected: contemporary biometrics often uses automated AI and machine learning techniques to detect and predict user behavior. This constrains individuals in their privacy and agency to self-determine how their biometric information is being used. AI, IoT, augmented and virtual reality settings and the related increase in remote sensor technology will likely aggravate these problems (Gordon et al. 2021). On the longer run, individuals may become increasingly hampered in freely deciding about the use of information concerning their identities and their human body. Hence, a violation of your privacy then might automatically imply a violation of the integrity of your body and your dignity.

4. Concluding remarks

As shown, biometrics is more than yet-another-identification technology: it has a substantial impact on embodiment and how humans use and are used by technology. The extended use of biometric information has consequences for its persistence and durability. Given the identifiable nature and irreversibility of biometric features, every interaction involving biometrics conveys strong identifiability of the person. This paper thus argues that the ongoing expansion of biometrics entails far-reaching sociotechnical shifts which imply a significant expansion of identifiability of individuals with substantial consequences on human rights and the role of technology in society. This development is yet underestimated in public discourse as well among policy makers and requires a broader societal debate and regulatory measures to reduce the corresponding risks. More precisely, because: 1) biometric information is bound to human bodies and thus irreversible, which makes individuals more vulner-

able to misuse; 2) the shift from a security towards a broadly used convenience technology fosters habituation effects and an incremental compulsion to provide biometric features; 3) the extensive use of biometric systems facilitates misuse, undermines secure processing of biometric information, reinforces surveillance tendencies, security risks and data protection issues; 4) biometrics used as automated control technology seriously strain human rights as it reinforces risks of discrimination and increasingly affects human dignity.

In the past, biometric technology was basically framed and used as security and surveillance technology in a limited number of application contexts. Extended usage was controversially discussed among researchers, policy makers, private and public stakeholders along the thin line between security governance and surveillance. However, during the last decade, a significant shift occurred where biometrics became partially re-framed – towards a commercial convenience technology increasingly embedded in various domains of everyday life. This development fosters habituation effects as people get more used to providing their biometric features. Different but interrelated economic and political drivers stimulate this development to make biometrics a mainstream technology for identification of individuals in public and private services, online and mobile applications and in law enforcement. This global trend to further broaden the use of biometrics and alleged gains in security and convenience make the surveillance capacity and manifold risks of this technology less obvious. This can lead to an incremental obligation to biometric identification which is already observable in some contexts (e.g., in banking or payment apps, digital wallets etc.) where non-biometric alternatives decrease. Moreover, with the increasing trend to distant biometric identification like facial recognition, individuals are widely exposed to biometric surveillance and related risks of social sorting and discrimination.

Beyond common surveillance practices, biometrics is a very substantial and expansive control technology reinforcing the excursion of institutional power over human bodies. On a more general level, the extensive use of biometrics is a form of power entanglement through technology. Its growing diffusion aggravates a core problem of digital identification (Strauß 2019): expanding information asymmetries between individuals and institutional actors implementing, performing and governing identification. This makes biometrics a highly intrusive technology which raises a number of societal and ethical issues. The broader the use of biometric features over different application contexts becomes, the more biometric systems may turn into a global assemblage of potentially interconnected ID systems. This is a crucial issue and a main reason for the highly intrusive nature of biometric technology: although there is no global biometric ID system, there is a serious risk, that the increasing use of biometrics leads to a blurry conglomerate of different but interwoven political control practices.

On the longer run, biometrics as mainstream technology may stimulate a reductionistic framing of individuals over their biometric information as commodified objects of control for political and economic purposes. In this framing, the individual is at risk to become reduced to a set of biometric features which serve as a sort of currency, e.g., to trade bodily information for gaining access to services or obtaining particular rights. One may argue that identity information was ever used in this regard. However, it is different with biometrics as you can never opt-out from your body. The simple reason for this lies in the irreversibility of biometric features and its inevitable linkage to the body. This also affects the vulnerability of individuals as their biometric features can be misused and are, in contrast to other forms of

identity information, not easily revocable and changeable. Hence, abuse can be very harmful, particular for individual persons. Biometrics is often not as secure as promoted and its usage only makes sense in very clearly defined, safe environments where misuse is very unlikely but not as mainstream technology. The growing cases of security breaches, attacks on biometric systems, of privacy violations and other forms of data abuse underlines that a further expansion of biometrics entails serious societal threats.

Expansion is also likely because biometrics is closely connected to AI-based technology and other forms of automated systems interacting with humans. These technologies basically use digital sensors to gain information about their environment and whenever interaction involves humans, biometrics is involved (e.g., via facial or voice recognition etc.). Technological trends like the IoT, as well as augmented and mixed realities imply a further increase in embedded sensors and biometric identification practices. Hence, an extensive growth in systems gathering and processing bodily features can be expected. If this expansion proceeds, the consequences for society and democracy can be severe: a further erosion of anonymity, privacy and related human rights, decreasing autonomy, agency and self-determination, increasing risks of data and security breaches like identity theft, increasing risks of social sorting, discrimination, and decreasing rights concerning bodily integrity and human dignity.

To circumvent these urges for a thorough societal debate on the risks of biometrics and stricter regulation of its usage contexts. Explicit prohibition is a blurry legal debate. Although the GDPR basically treats biometric data as sensitive, stronger protection is hampered by several gray areas in policy and legal regulations. Art. 9 of the GDPR prohibits the processing of biometric data the purpose of uniquely identifying natural persons. However, as biometrics are coupled to the human body and thus to the identity of a person, it is hardly avoidable that biometrics serve identification purposes. In practice, this is indistinct and mostly remains undetected. For instance, the extent to which facial images or photos (e.g., selfies) provide biometric information is often unclear. This facilitates unethical practices of data gathering as the outlined cases of Pimeyes and Clearview AI highlight. A legal clarification that facial images need protection from misuse as they can provide biometric information would contribute to ease this situation. A pressing issue concerns the increasing risk of discrimination based on biometric recognition which underlines the need for more effective rights against discrimination through technology and the strengthening of rights concerning human dignity and the integrity of the body. Given the enormous risks of a broad use of biometrics not just for abuse but for an erosion of democracy suggests the prohibition of commercial use of biometrics with accordingly high sanctions in case of abuse. This would contribute to make abuse less attractive. If society fails to tame the current proliferation of biometric systems, related business models and political power claims, in a not-so-distant future, anonymity might be diminishing and the inviolability of human dignity reduced to a statistical score.

Notes

[1] Induced by the ICAO (the International Civil Aviation Organization), a sub-unit of the United Nations.

[2] Regulation on electronic identification and trust services for electronic transactions in the internal

market (https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation).

[3] Payment Services (PSD 2) Directive (https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en).

[4] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation).

[5] The Prüm Convention (also known als Schengen III Agreement) is a European law enforcement treaty signed on May 27 2005 in the city of Prüm in Germany. It regulates data exchange for law enforcement (https://en.wikipedia.org/wiki/Pr%C3%BCm_Convention). Since 2020, plans foresee a significant extension of data exchange regulated by this legal framework (see EP 2020).

[6] One Trust Data Guidance, *Baden-Württemberg: LfDI Baden-Württemberg initiates proceedings against PimEyes to determine GDPR compliance* (May 28, 2021). Available at: https://www.dataguidance.com/news/baden-w%C3%BCrttemberg-lfdi-baden-w%C3%BCrttemberg-initiates.

References

Adler, Andy and Schuckers, Stephanie (2009) *Biometric Vulnerabilities, Overview*, in Stan Z. Li and Anil K. Jain (eds.), *Encyclopedia of Biometrics*, Boston, Springer, pp. 160-168.

Amoore, Louise (2011) *Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times*, in "Theory, Culture & Society", 28(6), pp. 24-43.

Arthur, Charles (2013, September 23) *iPhone 5S fingerprint sensor hacked by Germany's Chaos Computer Club*. The Guardian. Available at: www.theguardian.com/technology/2013/sep/22/apple-iphone-fingerprint-scanner-hacked (retrieved May 10, 2023).

Ball, Kirstie, Haggerty, Kevin D. and Lyon, David (2012) (eds.) *Handbook on Surveillance Studies*, Abingdon/New York, Routledge.

Barad, Karen (2007) *Meeting the Universe Halfway: Quantum Physics and the Entanglement of Matter and Meaning*, Durham & London, Duke University Press.

Bennett, Colin J. and Lyon, David (2008) (eds.) *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*, London/New York, Routledge.

Bijker, Wiebe E., Hughes, Thomas P. and Pinch, Trevor (1989) (eds.), *The Social Construction of Technological Systems: New Direction in the Sociology of Technology*, Cambridge, MA, MIT Press, 2008.

Bonneau, Vincent, Probst, Laurent and Lefebvre, Virginie (2018, January) *Biometrics technologies: A key enabler for future digital services*. Digital Transformation Monitor. Available at: https://ati.ec.europa.eu/reports/technology-watch/biometrics-technologies-key-enabler-future-digital-services (retrieved May 10, 2023).

Brewster, Thomas (2022, February 3) *Clearview: Glasses With Facial Recognition Are Here – And The Air Force Is Buying*. Forbes. Available at: https://www.forbes.com/sites/thomasbrewster/2022/02/03/clearview-ai-glasses-with-facial-recognition-are-here-and-the-air-force-is-using-them/ (retrieved May 10, 2023).

Burgess, Matt (2018, May 4) *Facial recognition tech used by UK police is making a ton of mistakes*. Wired. Available at: https://www.wired.co.uk/article/face-recognition-police-uk-south-wales-met-notting-hill-carnival (retrieved May 10, 2023).

Burt, Chris (2021, September 9) *Carmakers unveil biometrics plans as market forecast to surpass $700M by 2027*. Biometric Update. Available at: https://www.biometricupdate.com/202109/carmakers-unveil-biometrics-plans-as-market-forecast-to-surpass-700m-by-2027 (retrieved May 10, 2023).

Castelvecchi, Davide (2020) *Is facial recognition too biased to be let loose?*, in "Nature", 587(7834), pp. 347-349.

Christl, Wolfie (2017, June) *Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions*. Cracked Lab – Institute for Critical Digital Culture. Available at: https://crackedlabs.org/en/corporate-surveillance (retrieved May 10, 2023).

Clarke, Roger (2001) *Biometrics and Privacy*. Available at: http://www.rogerclarke.com/DV/Biometrics.html (retrieved May 10, 2023).

Clarke, Roger (2002) *Biometrics' Inadequacies and Threats, and the Need for Regulation*. Available at: http://www.rogerclarke.com/DV/BiomThreats.html (retrieved May 10, 2023).

Dong, Xingbo, Park, Jaewoo, Jin, Zhe, Teoh, Andrew B.J., Tistarelli, Massimo and Wong, KokSheik (2020) *On the Risk of Cancelable Biometrics*, in "arXiv: Computer Vision and Pattern Recognition" (preprint).

EDPB – European Data Protection (2022, March 10) *Board Facial recognition: Italian SA fines Clearview AI EUR 20 million*. Available at: https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en (retrieved May 10, 2023).

EDRi – European Digital Rights (2022, September 7) *Respecting fundamental rights in the cross-border investigation of serious crimes: A position paper by the European Digital Rights (EDRi) network on the European Union's proposed Regulation on automated data exchange for police cooperation ("Prüm II")*. Available at: https://edri.org/wp-content/uploads/2022/10/EDRi-position-paper-Respecting-fundamental-rights-in-the-cross-border-investigation-of-serious-crimes-7-September-2022.pdf (retrieved May 10, 2023).

EDRi – European Digital Rights (2021, March 24) *EDRi challenges expansion of police surveillance via Prüm*. Available at: https://edri.org/our-work/edri-challenges-expansion-of-police-surveillance-via-prum/ (retrieved May 10, 2023).

Eisenstein, Paul A. (2018, December 27) *No car keys? No problem. Hyundai rolls out fingerprint technology that makes keys as outdated as a landline*. CNBC. Available at: https://www.cnbc.com/2018/12/26/no-car-keys-no-problem-hyundai-rolls-out-fingerprint-technology.html (retrieved May 10, 2023).

EPIC – Electronic Privacy Information Center (2018) *Patel v. Facebook: US Court of Appeals for the Ninth Circuit*. Available at: https://epic.org/documents/patel-v-facebook/ (retrieved May 10, 2023).

Eveleth, Rose (2018, December 12) *Google Glass Wasn't a Failure: It Raised Crucial Concerns*. Wired. Available at: https://www.wired.com/story/google-glass-reasonable-expectation-of-privacy/ (retrieved May 10, 2023).

Farr, William, Price, Sara and Jewitt, Carey (2012) *An Introduction to Embodiment and Digital Technology Research: Interdisciplinary Themes and Perspectives*, NCRM – National Centre for Research Methods Working Paper, 02/12.

Feenberg, Andrew (2002) *Transforming Technology: A Critical Theory Revisited*, New York, Oxford University Press.

FIDO Alliance – Fast IDentity Online (2022, May 5) *Apple, Google and Microsoft Commit to Expanded Support for FIDO Standard to Accelerate Availability of Passwordless Sign-Ins*. Available at: https://fidoalliance.org/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard-to-accelerate-availability-of-passwordless-sign-ins/ (retrieved May 10, 2023).

Field, Hayden (2021, November 5) *Facebook shut down its facial-recognition tech, but left Meta's door open*. Tech Brew. Available at: https://www.emergingtechbrew.com/stories/2021/11/05/facebook-shut-down-its-facial-recognition-tech-but-left-meta-s-door-open (retrieved May 10, 2023).

Foltýn, Tomáš (2019, January 10) *Face unlock on many Android smartphones falls for a photo*. WeLiveSecurity. Available at: https://www.welivesecurity.com/2019/01/10/face-unlock-many-android-smartphones-falls-photo/ (retrieved May 10, 2023).

FRA – European Union Agency for Fundamental Rights (2021, January 8) *EU Charter of Fundamental Rights*. Available at: https://fra.europa.eu/en/eu-charter (retrieved May 10, 2023).

French, Martin, and Smith, Gavin JD (2016) *Surveillance and Embodiment: Dispositifs of Capture*, in "Body & Society", 22(2), pp. 3-27.

Gomez-Barrero, Marta and Galbally, Javier (2020) *Reversing the irreversible: A survey on inverse biometrics*, in "Computers & Security", 90, 101700.

Gordon, Jeremy R., Curran, Max T., Chuang, John and Chesire, Coye (2021) *Covert Embodied Choice: Decision-Making and the Limits of Privacy Under Biometric Surveillance*, in "Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)", 551, pp. 1-12.

Grother, Patrick J., Ngan, Mei L. and Hanaoka, Kayee K. (2019, December) *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*. NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology. Available at: https://www.nist.gov/publications/face-recognition-vendor-test-part-3-demographic-effects (retrieved May 10, 2023).

Hadid, Abdenour, Evans, Nicholas, Marcel, Sébastien and Fierrez, Julian (2015) *Biometrics systems under spoofing attack: An evaluation methodology and lessons learned*, in "IEEE Signal Processing Magazine", 32(5), pp. 20-30.

Haggerty, Kevin D. and Ericson, Richard V. (2000) *The Surveillant Assemblage*, in "British Journal of Sociology", 51(4), pp. 605-622.

Hill, Kashmir (2020a, January 18) *The Secretive Company That Might End Privacy as We Know It*. The New York Times. Available at: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (retrieved May 10, 2023).

Hill, Kashmir (2020b, June 24) *Wrongfully Accused by an Algorithm*. The New York Times. Available at: https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html (retrieved May 10, 2023).

Hill, Kashmir (2021, December 29) *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*. The New York Times. Available at: https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html (retrieved May 10, 2023).

HRW – Human Rights Watch (2021) *Russia: Broad Facial Recognition Use Undermines Rights*. Available at: https://www.hrw.org/news/2021/09/15/russia-broad-facial-recognition-use-undermines-rights (retrieved May 10, 2023).

Jain, Anil K., Nandakumar, Karthik and Ross, Arun (2016) *50 years of biometric research: Accomplishments, challenges, and opportunities*, in "Pattern Recognition Letters", 79, pp. 80-105.

Ken Paxton Attorney General of Texas (2022, February 14) *Paxton Sues Facebook for Using Unauthorized Biometric Data* (press release). Available at: https://www.texasattorneygeneral.gov/news/releases/paxton-sues-facebook-using-unauthorized-biometric-data (retrieved May 10, 2023).

Koebler, Jason (2020, June 29) *Detroit Police Chief: Facial Recognition Software Misidentifies 96% of the Time*. Motherboard – Tech by VICE. Available at: https://www.vice.com/en/article/dyzykz/detroit-police-chief-facial-recognition-software-misidentifies-96-of-the-time (retrieved May 10, 2023).

Kruzan, Kaylee P. and Won, Andrea S. (2019) *Embodied well-being through two media technologies: Virtual reality and social media*, in "New Media & Society", 21(8), pp. 1734-1749.

Laufer, Daniel and Meineck, Sebastian (2020, July 10) *Pimeyes: A Polish company is abolishing our anonymity*. Netzpolitik. Available at: https://netzpolitik.org/2020/pimeyes-face-search-company-is-abolishing-our-anonymity/ (retrieved May 10, 2023).

Leyden, John (2016, October 5) *Mastercard rolls out pay-by-selfie across Europe*. The Register. Available at: https://www.theregister.com/2016/10/05/mastercard_selfie_pay (retrieved May 10, 2023).

Lyon, David (ed.) (2003) *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*, London, Routledge.

Lyon, David (2008) *Biometrics, identification and surveillance*, in "Bioethics", 22(9), pp.499-508.

Magnet, Shoshana A. (2011) *When Biometrics Fail: Gender, Race, and the Technology of Identity*, Durham and London, Duke University Press.

Maguire, Mark (2009) *The birth of biometric security*, in "Anthropology Today", 25(2), pp. 9-14.

Malhotra, Ashish (2018, January 8) *The World's Largest Biometric ID System Keeps Getting Hacked*. Motherboard – Tech by VICE. Available at: https://www.vice.com/en/article/43q4jp/aadhaar-hack-insecure-biometric-id-system (retrieved May 10, 2023).

Meloncon, Lisa (ed.) (2013) *Toward a Theory of Technological Embodiment*, in *Rhetorical Accessability: At the Intersection of Technical Communication and Disability*, New York, Routledge, pp. 67-81.

Mordini, Emilio and Tzovaras, Dimitros (eds.) (2012) *Second Generation Biometrics: The Ethical, Legal and Social Context*, Dordrecht, Springer.

Ng, Alfred (2020, August 11) *How China uses facial recognition to control human behavior*. CNet. Available at: https://www.cnet.com/news/politics/in-china-facial-recognition-public-shaming-and-control-go-hand-in-hand/ (retrieved May 10, 2023).

Oracle (2014, December 22) *Oracle Buys Datalogix: Creates the World's Most Valuable Data Cloud to Maximize the Power of Digital Marketing*. Available at: https://www.oracle.com/corporate/press-release/oracle-buys-datalogix-122214.html (retrieved May 10, 2023).

Perez, Sarah (2021, June 4) *TikTok just gave itself permission to collect biometric data on US users, including "faceprints and voiceprints"*. TechCrunch. Available at: https://techcrunch.com/2021/06/03/tiktok-just-gave-itself-permission-to-collect-biometric-data-on-u-s-users-including-faceprints-and-voiceprints/ (retrieved May 10, 2023).

Ramachandra, Raghavendra and Busch, Christoph (2017) *Presentation Attack Detection Methods for Face Recognition Systems: A Comprehensive Survey*, in "ACM Computing Surveys", 50(1), pp. 1-37.

Rao, Ursula and Nair, Vijayanka (2019) *Aadhaar: Governing with Biometrics*, in "South Asia: Journal of South Asian Studies", 42(3), pp. 469-481.

Sayer, Peter (2013, March 4) *Fujitsu names UniCredit as first European customer for palm-scan authentication*. Network World. Available at: https://www.networkworld.com/article/2164100/fujitsu-names-unicredit-as-first-european-customer-for-palm-scan-authentication.html (retrieved May 10, 2023).

Schaber, Felix, Strauß, Stefan and Peissl, Walter (2020) *Der Körper als Schlüssel? Biometrische Methoden für Konsument*innen*, Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften, Wien.

Schneier, Bruce (1999) *Inside Risks: The Uses and Abuses of Biometrics*, in "Communications of the ACM", 42(8), p. 136.

Smith, Gavin JD (2016) *Surveillance, Data and Embodiment: On the Work of Being Watched*, in "Body & Society", 22(2), pp. 108-139.

Strauß, Stefan (2019) *Privacy and Identity in a Networked Society: Refining Privacy Impact Assessment*, Abingdon/New York, Routledge.

Strzyżyńska, Weronika (2022, September 5) *Iranian authorities plan to use facial recognition to enforce new hijab law*. The Guardian. Available at: https://www.theguardian.com/global-development/2022/sep/05/iran-government-facial-recognition-technology-hijab-law-crackdown (retrieved May 10, 2023).

Tarabay, Jamie (2021, September 22) *Chinese Hackers Targeted Aadhaar Database, Times Group: Report*. NDTV. Available at: https://www.ndtv.com/india-news/chinese-hackers-targeted-aadhaar-database-times-group-report-2549166 (retrieved May 10, 2023).

Titchkosky, Tanya (2007) *Reading and Writing Disability Differently: The Textured Life of Embodiment*, Toronto, University of Toronto Press.

Vavoula, Niovi (2020, September) *Police Information Exchange: The future developments regarding Prüm and the API Directive*. European Parliament. Available at: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2020)658542 (retrieved May 10, 2023).

Zuboff, Shoshana (2019) *The Age of Surveillance Capitalism: The Fight for Future at the New Frontier of Power*, London, Profile Books.