ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 3 (March)
http://doi.org/10.9770/jesi.2023.10.3(10)

Publisher
http://jssidoi.org/esc/home

THE USE OF BIOMETRIC TECHNOLOGIES IN ENSURING THE SECURITY OF CRITICAL INFRASTRUCTURE: THE CONTEXT OF THE PROTECTION OF PERSONAL DATA*

Darius Štitilis [1], Marius Laurinaitis [2], Egidijus Verenius [3]

[1,2] Mykolas Romeris University, Ateities st. 20, Vilnius, Lithuania
[3]State Data Protection Inspectorate, L. Sapiegos st. 17, Vilnius, Lithuania

E-mails: [1]stitilis@mruni.eu; [2]laurinaitis@mruni.eu; [3]egidijus.verenius@ada.lt

Received 11 November 2022; accepted 8 February 2023; published 30 March 2023

Abstract. The article examines aspects of the use of biometric technologies and the protection of personal data as it relates to the protection of critical infrastructure in the state. The use of biometric technologies for the protection of critical infrastructure is examined in this article through employee identification to establish the identity of employees unequivocally, for example, when entering such infrastructure facilities. The EU General Data Protection Regulation (GDPR) sets specific conditions for processing biometric data. Still, the relevant data controllers often have problems finding the appropriate basis for processing, especially in the context of GDPR Article 9. The authors, having examined the conditions for the processing of biometric data, propose introducing a particular legal framework for the processing of biometric data as far as it relates to the protection of critical infrastructure.

Keywords: General Data Protection Regulation; data protection; biometric technologies; protection of critical infrastructure; processing of biometric data; identification; legal regulation

Reference to this paper should be made as follows: Štitilis, D., Laurinaitis, M., Verenius, E. 2023. The use of biometric technologies in ensuring critical infrastructure security: the context of protecting personal data. *Entrepreneurship and Sustainability Issues*, 10(3), 133-150. http://doi.org/10.9770/jesi.2023.10.3(10)

JEL Classifications: J53, J58

Additional disciplines: law

1. Introduction

Acknowledging that any nation's national and economic security depends on the reliable functioning of critical infrastructures (CIs), the CIs are now more at risk than ever. Today's critical infrastructures, including healthcare, government and other essential sectors, are highly digitised and sometimes interconnected, placing them firmly in the sights of threats (Roshanaei, 2021). One of which is cyber threats. Statistics on cyber threats against critical infrastructure show that such attacks are rising (Weinberg, 2021). The dependence of people and society on

* *This article was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020)*

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 3 (March)
http://doi.org/10.9770/jesi.2023.10.3(10)

critical infrastructure and the probability and potential consequences of this infrastructure being vulnerable are the reasons that encourage individual criminals or criminal groups to attack these infrastructures and test their cyber resilience (Weinberg, 2021).

While there are no universally accepted definitions for the terms critical infrastructure and critical information infrastructure, and governments must consider which entities and services to include based on their national risk assessment (National Cybersecurity Strategy Good Practice), there is still no doubting the importance of protecting critical infrastructure. Critical infrastructure is crucial for any society to survive (Baggott & Santos, 2020; Roshanaei, 2021).

Attempts to affect critical infrastructure are usually made externally. Still, as security systems improve, there may be more and more attempts to affect these infrastructures and cause significant cyber incidents by way of the weakest point – humans. The human element of a system cannot be underestimated or easily understood. Insider human threats, such as those by disgruntled employees, fall within the human head topic (Zimmerman, 2017; Baggott & Santos, 2020). Hence, not only external threats to critical infrastructure should be emphasised – internal threats should be as well. Identifying internal employees or other related persons entering the relevant infrastructure facilities is crucial. And biometric technologies offer a highly effective means of identifying individuals. Biometrics has become part of the landscape of business and organisations (North-Samardzic, 2020). Despite this, the legal framework for personal data regulation strongly limits the use of biometric technologies (Kindt, 2018; Smith & Miller, 2022). Next, this article analyses the relevant legal framework based on the EU General Data Protection Regulation and the possibility of using biometric technologies to protect critical infrastructure.

Several methods were used for the research. An empirical method of analysis of legal documents, case law, and decisions and opinions of the state institutions responsible for data protection was used to determine the relevant legal regulation in force. This method makes it possible to accurately identify and describe the applicable legal regulation of the relationship in question after examining official documents. The authors used the comparison method when analysing the information published by different institutions. For sources of scientific literature, the authors used the deduction method, allowing for sufficiently reliable conclusions. Historical and analytical methods were also used.

2. The need for critical infrastructure protection

Critical infrastructures are vital for public safety, economic well-being and national security (Maglaras, Janicke & Mohamed, 2022). Researchers from different countries have attempted to look for an effective cyber-security model. In their view, ensuring cooperation on critical infrastructure cyber security is crucial at domestic and international levels. Destruction or malfunctioning due to a specific risk factor could endanger life as well as the operation of the state (Kruszka, Klósak & Muzolf, 2019).

Recently, an increase in cyber-attacks against critical infrastructures, especially power systems, has been reported. It was previously thought that the risk of cyber-attacks on critical infrastructures was low because of the need for specialist knowledge of the control system configuration and administrative operations and the absence of suitable Internet connections. However, cyber-attacks on critical infrastructures are now exerting a significant impact on society (An Analysis of the Actual Status of Recent Cyberattacks on Critical Infrastructures).

Cyber-attacks on critical infrastructures such as power systems have significant economic implications and risk becoming targets in conflicts between nations (An Analysis of the Actual Status of Recent Cyberattacks on Critical Infrastructures). Especially in the context of the military conflict between the Russian Federation and the independent state of Ukraine, the probability of such disputes is increasing even more, particularly in the

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 3 (March)
http://doi.org/10.9770/jesi.2023.10.3(10)

neighbouring countries of Eastern Europe. Research shows a massive threat from Russia, with Russian state-sponsored cybercrime groups (Cybersecurity & Infrastructure Security Agency, 2022). The cybercrime groups no longer hide that they are directly controlled and financed by Russian security services. The threat is not only to Ukraine. Some groups are threatening and conducting cyber operations against countries and organisations that provide material or other support to Ukraine (Cybersecurity & Infrastructure Security Agency, 2022). And there are many such countries. In this context, the countries that claim the most outstanding support for Ukraine are most at risk (Economist, 2022). Among these countries are the Baltic States, including Lithuania. Of course, threats to critical infrastructure can and do arise without any connection to the current geopolitical situation. This infrastructure has been the target of many criminals and criminal groups for decades.

Critical infrastructures are complex operating environments that often require special protection and security (Noguchi & Ueda, 2021; Tvaronavičienė et al., 2022). Most countries are amping up critical infrastructure protection. On 15 March 2022, President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act of 2022, which imposes federal reporting requirements for cyber incidents and ransomware attack payments (Cleary Gottlieb Steen & Hamilton LLP, 2022). Critical infrastructure protection is thus becoming one of the most important tasks for every country.

Cyber threats are divided into external and internal. Internal threats, i.e. threats to infrastructure security that originate from within, are often underestimated. Although in terms of consequences, these threats may not be inferior to external threats and may sometimes lead to more severe consequences. One example is the 1992 case at the Ignalina nuclear power plant in Lithuania when an internal employee – a technician – introduced a virus that nearly caused a nuclear disaster (Paganini, 2015). A global survey of security professionals and executives (LogRhythm, 2022) found that identity and access management are the most relevant security measures for organisations looking to close security gaps (Figure 1).

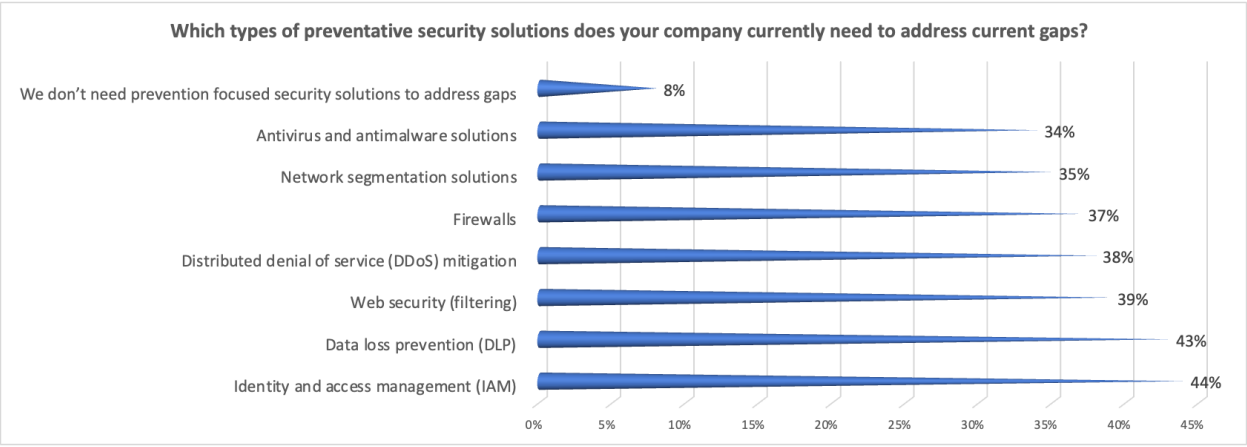

Figure 1. Identity and access management are the most relevant security measures for organisations
Source: LogRhythm, 2022

Biometric technologies offer a highly effective means of authenticating internal employees with access to critical infrastructure. These means could be one solution to protecting this infrastructure from internal cyber threats. However, using sensitive data brings several extra burdens (Quinn, 2021).

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 3 (March)
http://doi.org/10.9770/jesi.2023.10.3(10)

3. Market overview of biometric technologies and the need for data protection

The biometric technology market is constantly growing, with 2021 being a turning point in the development of the biometrics and cybersecurity market (Global Biometrics Market Report, 2021). Statista Inc. expects the biometric technology market to continue to grow over the next few years and to reach USD 68.6 billion by 2025 (Global biometric system market revenue in 2020 and 2025). The development and ease of use of biometric technologies and the COVID-19 pandemic, have encouraged financial institutions to use these technologies more actively for customer identification. Despite the limitations mentioned above of the technology and the known shortcomings of facial recognition technologies, companies worldwide are marketing such multimodal biometric technologies as practical tools in the fight against the pandemic. (Van Natta et al., 2020; Pascu, 2020) According to forecasts from Statista Inc., worldwide spending in the identity verification market will grow by more than USD 13 billion (from 4.93 billion in 2017 to over 18 billion in 2027) (Identity verification market, 2022) (Global Biometrics Market Report, 2021). Researchers in computer and technology ethics have made valuable contributions, but the implications of biometrics are not their primary ethical concern. As organisations are a place the development and deployment of biometric technologies and biometrics can present unique ethical challenges, it would be helpful for the community to focus on this topic more attention (North-Samardzic, 2020).

The following fastest-growing biometric technology markets can be singled out:

- The facial recognition market: The bulk of facial recognition on intelligent devices will be software-based rather than hardware-based, with over 1.3 billion devices having this capability by 2024 (i-SCOOP, n.d.). The facial recognition market is projected to grow from USD 5 billion in 2021 to USD 12.67 billion by 2028 (Statista, Facial recognition market size worldwide, 2019). COVID-19 accelerated progress in the facial recognition market – the sudden need to recognise a face partially covered by a mask prompted the development of new face recognition algorithms (Hernández A., 2020).
- The voice recognition market: The global voice recognition market size is forecast to grow to USD 27.16 billion by 2026 (from 10.7 billion in 2020) (Voice recognition market, 2023). The use of these technologies in the automotive industry is rapidly growing, with voice assistants projected to be embedded in nearly 90% of new vehicles sold globally by 2028. Amazon, Google, Nuance and IBM are all pushing hard to become the leading service providers for this industry. How well the in-vehicle systems integrate into smartphones and home automation will be a crucial factor to success (Abuelsamid, 2019).
- The fingerprint recognition market: Of all mobile devices sold in 2018, 96.5% had fingerprint recognition technology installed. Fingerprint hardware will dominate biometric payments, with more than 4.6 billion smartphones estimated to be equipped with fingerprint sensors by 2024 (Market share of smartphone fingerprint, Statistica 2023).
- eIDAS (electronic Identification, Authentication and Trust Services): The global digital signature market size is projected to grow from USD 4.0 billion in 2021 to USD 16.8 billion by 2026. Demand for digital signatures is expected to grow significantly, since e-government services, e-commerce markets, the need for security, and the number of electronic contracts are all increasing worldwide (MarketandMarkets, 2022). Password-based digital signature services are looking for added levels of protection, and biometric technologies are helping to make this happen. New biometric signatures consist of authentication via fingerprints, retinal identification, iris recognition, facial recognition or voice recognition and a record of the will of the person signing.
- Personal data breaches and cybersecurity: Human error and weak passwords (even passwords that are changed frequently can create opportunities for personal data breaches) mean that the latest biometric technologies must replace traditional authentication methods. Consumers are more concerned about the rise of cybercrime but are unable to protect themselves. As many as 92% of people know that reusing the

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 3 (March)
http://doi.org/10.9770/jesi.2023.10.3(10)

same passwords across multiple online accounts puts them at risk of password theft, yet 65% of users still do so (Psychology of Passwords, 2022).

Biometric identification and authentication are used in various fields and for multiple purposes. Banks and finance are particularly relevant areas for us. Financial institutions use biometric technology as a multi-factor authentication tool to protect themselves and their customers from fraud attacks. Whether it is the financial institutions themselves or their customers, biometric data benefit everyone in the financial sector – it allows for fast and accurate customer identification, protection from fraud, increased mobile banking security, and lower IT and customer service costs (when identification instruments are lost). In an official response to the question of strong customer authentication and common and secure communication (incl. access) in 2019, the European Banking Authority noted that financial institutions might use biometric data stored at the device level for the application of strong customer authentication, provided that they have ensured that the technology has a sufficient level of security (Relying on vendor mechanisms processing, 2019). The fact is that proper identification of customers in the physical space is becoming almost impossible, and the only means of resisting this type of attack (when foreign identity documents are used in the physical space) is to use biometric identification (Report on existing remote onboarding solutions in the banking sector, 2019). Research shows that services related to biometric sensors will include ATMs, e-mail banking, facial recognition systems, voice recognition services, optical sensors, fingerprint recognition and facial recognition services. Biometric systems will require two forms of authentication, including biometric data along with a personalised security number (PIN) will make designs more robust and secure (Dauda & Lee, 2015). Another new and breakthrough level of identification is EEG-based (electroencephalography) biometric data. EEG identification is a suitable alternative to existing personal identification methods, ensuring a high level of security. Several studies have shown that EEG-based identification and authentication systems can provide high recognition accuracy and stability (Chan et al., 2018).

Another equally important area is healthcare. Biometric identification can help hospitals confirm a patient's identity and ensure that medical staff access the correct medical records. A European Union-funded innovation project called Panacea (Panacea, n.d.) shows biometric access control software tools that would be a part of a healthcare identity management platform. The tool kit for human-to-machine and machine-to-machine interfaces includes software for secure information sharing, dynamic risk assessment, security by design support and compliance. According to market forecasts, by 2024, biometrics in the healthcare sector will generate four times more revenue. E-health systems and Internet of Things-based healthcare solutions will drive the adoption of biometric technologies. Biometric systems such as behavioural biometrics, cognitive recognition and wearables are being developed due to their advantages in remote monitoring and diagnostic healthcare services. Multilayer biometrics will strengthen the implementation of biometric technologies and ensure excellent resistance to personal data theft and falsification in the healthcare sector (Healthcare: Global Market Trends for Biometrics, 2020). As an example, it can be mentioned that the use of biometric solutions at airports will significantly reduce contact with all passenger touchpoints, such as at the check-in desk (including baggage drop), border customs procedures, and boarding process, which will help to apply effective health protection measures at airports during potential health crises (Serrano & Kazda, 2020).

Another critical sector is law enforcement. Law-enforcement authorities use several types of biometric technology for identification. These include fingerprints, facial recognition, voice recognition and DNA. There are many ethical questions regarding using biometric identification methods in the public domain. Questions arise about technologies specifically related to biometrics and those related to large-scale surveillance of individuals. Questions arise about the purposes for which this technology is used and how it is used (Wendehorst & Duller, 2021).

Thus, biometric technologies and their use have developed in some sectors. The question is how these technologies can be used to identify and authenticate critical infrastructure employees.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 3 (March)
http://doi.org/10.9770/jesi.2023.10.3(10)

4. The use of biometric technologies in EU Member States: Legal regulation and practice

The GDPR sets the general rules for processing biometric data in EU Member States. Biometric data are defined in the GDPR 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 dactyloscopy data* (Article 4(14)). GDPR Article 9(1), which regulates the processing of special categories of personal data, states that *the processing of ... biometric data to identify a natural person uniquely... shall be prohibited*.

When systematically evaluating these provisions of the GDPR, two scenarios for the use of biometric technologies can be distinguished: (1) the use of biometric technology not to identify a natural person uniquely, and, conversely, (2) the use of biometric technology to identify a natural person uniquely. Thus, it seems that the biometric technology chosen will determine which GDPR rules will apply, i.e. if the processing of biometric data will be subject to the conditions of lawful personal data processing set out in GDPR Article 6, or if it will also be subject to the exceptions to the processing of special categories of personal data set out in GDPR Article 9.

This is the approach taken by the European Data Protection Board after interpreting that to qualify as biometric data as defined in the GDPR, the processing of raw data, such as the physical, physiological or behavioural characteristics of a natural person, must imply measurement of these characteristics. Biometric data are the result of such measures. However, video footage in which a person is visible can only be considered biometric data if it has been technically processed to help identify the person. For biometric data to be considered as processing of special categories of personal data, they must be processed "to uniquely identify a natural person" (European Data Protection Board, Guidelines 3/2019).

4.1 Examples of legal regulation on the processing of biometric data in the national law of EU Member States

Various examples of legal regulation on the processing of biometric data in the law of EU Member States. In Hungary, numerous pieces of legislation regulate the processing of biometric data. The Labour Code provides that an employee's biometric data may be processed to prevent unauthorised access to an item or data that could cause severe or massive irreversible harm to the life, physical integrity or health of the employee or others, or to a significant interest protected by law. "Major interests protected by law" include information classified as "Confidential", as well as the safeguarding of weapons, toxic or nuclear materials (Act I of 2012 on the Labour Code). The processing of biometric data related to granting access is also provided for sports events. A sports event organiser can process biometric data using an access control system (Act I of 2004 on the Sport). The General Rules also cover the processing of biometric data for Trust Services and Electronic Payments, which specify that access to government-provided identification services, among other things, identification using video technologies, is permitted (Act CCXXII, 2015).

In Slovakia, the processing of biometric data to grant access is provided for gaining access to nuclear facilities (Act No. 541/2004). Slovakia has also developed a legal regulation for processing biometric voice data to verify the customer's identity when making payments and for other purposes provided for in the legislation (Act No. 483/2001).

Similar to Hungary or Slovakia, Italy permits the processing of biometric data for providing physical or logical access to data, provided that appropriate safeguards are in place (Code regarding the protection of personal data, 2016).

However, the practice of legal regulation for processing biometric data has yet to be widespread in individual EU Member States.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 3 (March)
http://doi.org/10.9770/jesi.2023.10.3(10)

4.2 The practice of GDPR supervisory authorities regarding the processing of biometric data

The supervisory authorities of the EU Member States have repeatedly assessed the compliance of the processing of biometric data with personal data protection rules. In its 2018 annual report, the Bulgarian supervisory authority stated that a bank had approached it regarding the processing of biometric voice data for customer identification purposes. The bank had planned to use biometric voice data with the customer's phone number and the last four digits of the active bank card number. In the opinion of the Bulgarian supervisory authority, this method chosen by the bank for identifying data subjects is only possible with the express written consent of the data subject, giving the option of selecting alternative forms of identification (Commission for Personal Data Protection, Bulgaria).

In 2019, the Swedish supervisory authority imposed an administrative fine on a school for using facial recognition technology for monitoring attendance. In the opinion of the Swedish supervisory authority, the use of such technology was disproportionate concerning the purpose. Furthermore, the consent of students and their parents cannot be collected because they cannot freely choose whether or not to be monitored (Swedish Authority for Privacy Protection, 2019).

In its 2020 annual report, the Irish supervisory authority described a case of biometric data processing at a secondary school. The school sought to process students' facial images for attendance monitoring purposes. According to the Irish supervisory authority, the use of such technologies must have a clear legal basis and justification because otherwise, it can desensitise students to such technology and lead to them ceding their data protection rights in other contexts as well (Data Protection Commission, 2020).
The supervisory authorities of the EU Member States have also investigated possible violations of the legal regulation of personal data protection in processing employees' biometric data. The Romanian supervisory authority investigated a possible violation regarding facial biometric data of employees that were being processed for timekeeping purposes. The Romanian supervisory authority decided that such processing of biometric data is unlawful because it is disproportionate in relation to the purpose. The organisation could have achieved its goals with less privacy-intrusive means (The National Supervisory Authority for Personal Data Processing, 2018).

Several cases were investigated by supervisory authorities that resulted in administrative fines involving using employee fingerprints.

In 2021, the Italian supervisory authority imposed an administrative fine on a data controller for processing employee fingerprints to ensure control of employees' presence at work. In the opinion of the Italian supervisory authority, this processing was disproportionate concerning the purpose. It had no legal basis (Injunction Order against the Provincial Health Authority of Enna, 2021).

The Lithuanian and Spanish supervisory authorities have imposed administrative fines for processing employees' fingerprints for entry control. The decision of the Lithuanian supervisory authority was based on the fact that the data controller did not specify on what legal basis and for what purposes it was processing employees' fingerprints, nor did it assess the necessity and proportionality of such measures (Lithuanian DPA, 2021). Meanwhile, the Spanish supervisory authority based its decision to impose an administrative fine for the processing of employees' fingerprints for admission into premises because these objectives could be achieved by less privacy-intrusive means (Procedimiento Nº: PS/00010/2021).

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 3 (March)
http://doi.org/10.9770/jesi.2023.10.3(10)

From the examples given, it can be concluded that using biometric technologies for the authentication and identification of employees is often recognised as excessive or without a legal basis. Providing a legal basis through legal regulation could be a solution in cases identified by the state as significant enough to warrant biometric technologies.

5 Use of biometric technologies outside of the EU: Current practices and trends

5.1 The need for the use of biometric technologies

The need for the use of biometric technologies is common. It can also depend on the industry. For example, fingerprints are considered the most common in financial services and the government. Iris scanning technology is deemed more of a niche biometric tool used in high-security industries. Many workplaces take pictures of people regularly. These photos are then used to create company badges or identification (Robb, 2022). Yes, this method is not related to the use of biometrics. However, it is only a matter of time before employers want to use employee photos for identification, which would already involve using biometric technologies. But how easy will it be for the data controllers to lawfully switch to these technologies in more convenient ways?

Below is an analysis of the permissibility and legalisation of biometric technologies in some non-EU countries. The United States, Canada and Australia were selected for the study. Although GDPR Article 3 provides for the principle of territorial scope and the processing of personal data in these countries may be subject to the GDPR in some instances, these countries do not belong to the EU, and in a general sense, the policies of these countries regarding biometric technologies may differ from the EU. It is, therefore, valuable to analyse the practices of the respective countries regarding the use of biometric technologies, including at the workplace, as well as related trends.

5.2 Pros and cons of using biometric technologies

There is intense debate about the pros and cons of using biometric technologies. Canada is one of the countries where the advantages and disadvantages of using biometric technologies to process personal data are being considered. On the one hand, this is an ideal technology for "not forgetting your password" and the like. But on the other hand, biometric information is unique to each individual and remains relatively immutable. Accordingly, if a security breach results in the theft of the biometric data of one individual or thousands, managing the risk of harm to the said individual or individuals is not as simple as cancelling a credit card or changing a password. Therefore, it is considered that, despite a relatively liberal stance on new technologies, Canadian privacy legislation should be further clarified regarding the application of biometric technologies to manage the risks arising from using these technologies (Backman & Kennedy, n.d.).

The risks that exist were illustrated by a "discovery" made by two Israeli researchers. These researchers managed to access a database with the fingerprints of over one million people and facial recognition data that security company Suprema ordered on behalf of its clients across the globe (including police, defence contractors and banks). These researchers also showed that they could tamper with this data by adding their fingerprints to existing users or adding new users. Although it is uncertain whether the unsecured biometric data was, in fact, maliciously accessed and used, the most significant concern is that, unlike passwords, biometric data cannot be reset following a leak, and it is, therefore, challenging to mitigate the risk (Van Canneyt, 2019; Meden et al., 2021).

The Australian supervisory authority is strict about certain biometric technologies-related issues. After Canada, Australia also found that controversial facial recognition company Clearview AI had violated national privacy laws when it secretly collected facial biometric data from citizens and incorporated them into its AI-powered identity matching service, which it sells to law enforcement agencies and others (Lomas, 2021). In its report, the Australian supervisory authority states: "Clearview AI's facial recognition tool includes a database of more than

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 3 (March)
http://doi.org/10.9770/jesi.2023.10.3(10)

three billion images taken from social media platforms and other publicly available websites. The tool allows users to upload a photo of an individual's face and find other facial images of that person collected from the internet. It then links to where the photos appeared for identification purposes." (The Office of the Australian Information Commissioner, 2021) The ruling orders Clearview AI to cease collecting facial images and biometric templates from individuals in Australia and to destroy existing images and templates contained in Australia.

Surveys show that two-thirds (66%) of Australians are reluctant to provide biometric information to a business, organisation or government agency, and a quarter (24%) are more reluctant to provide biometric information than any other type of information. This is higher than an unwillingness to provide medical or health information (60% reluctant and 8% most reluctant) and location data (56% reluctant and 6% most reluctant) (The Office of the Australian Information Commissioner, 2020). Figure 2 below shows that Australian citizens are still largely opposed to the use of biometric information.

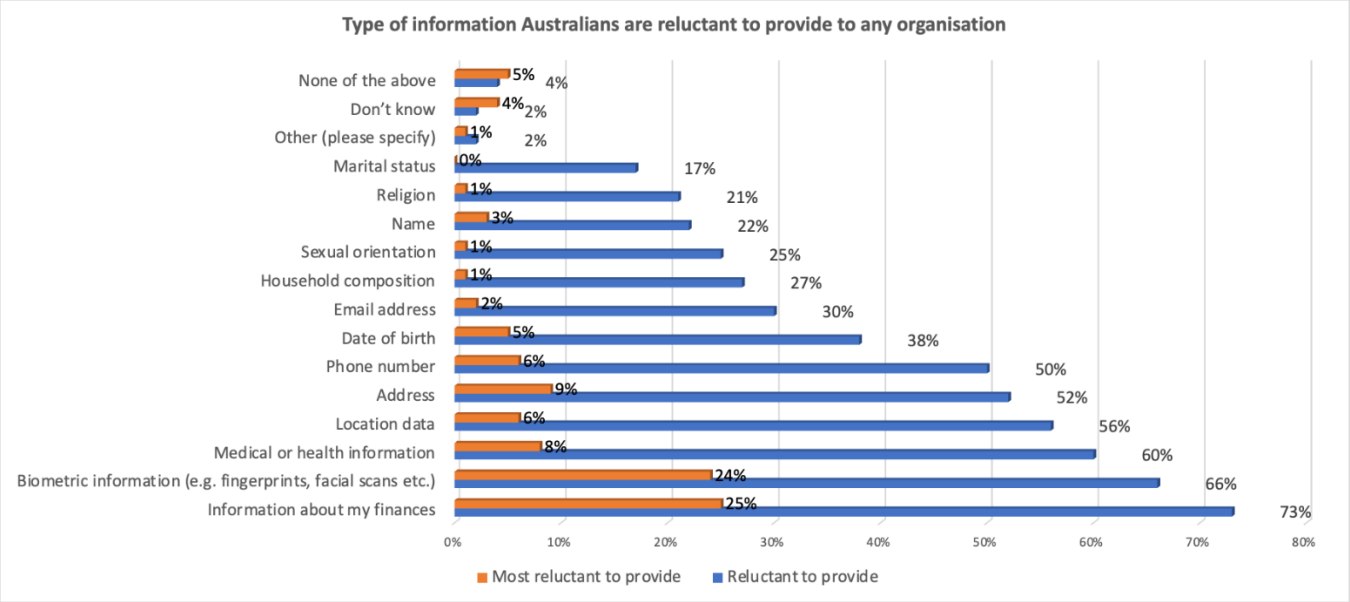

Figure 2. Type of information Australians are reluctant to provide to any organisation
Source: Office of the Australian Information Commissioner

In Canada, the immutability of biometric information is seen as both an advantage[†]; there are disadvantages too. Potential problems include the high risk of unauthorised disclosure, theft or misuse of biometric information. Accordingly, if a security breach results in the theft of the biometric data of one individual or thousands, managing the risk of harm to the said individual or individuals is not as simple as cancelling a credit card or changing a password. This highly sensitive information should be adequately protected from misuse and theft (Backman & Kennedy, n.d.). These problems are considered severe enough to be considered in legal regulation.

Given the risks involved, so-called "untraceable biometrics" has begun to be debated in Canada. In theory, untraceable biometric technologies are secure technologies that allow biometric information to be processed and used so that the biometric data are not linked to an identifiable person because biometric images or a biometric template does not store them. The original biometric data cannot be recovered from the stored information.

[†] There is a widespread belief that biometrics is ideal for identification or authentication purposes

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 3 (March)
http://doi.org/10.9770/jesi.2023.10.3(10)

Biometric data are provided in many ways that vary by technology. Personal data are converted in an irreversible and untraceable manner into an otherwise unrelated string of data, personal identification number (PIN) or key. When a person resubmits their biometric information, the unique PIN or key is regenerated and compared to the stored string. In essence, biometric data can be seen as a decoder for a unique PIN that allows a person to be identified (Cavoukian & Snijder, 2009). Untraceable biometrics are recognised as one of the solutions to the risks mentioned above. Nevertheless, this technology has yet to be thoroughly tested, and its use is limited (Backman & Kennedy, n.d.).

Canada is already beginning to see some solid official opinions on biometric technologies. In 2021, the Canadian supervisory authority found that a company that collected images of individuals and used facial recognition software violated privacy requirements. Following its joint investigation, the commissioners determined that Clearview's collection of more than three billion images – millions of which belong to Canadians – took place without the knowledge or consent of citizens. Additionally, the commissioners found that the company did not use and disclose the collected data adequately (IAPP, 2021).

5.3 Legal regulation related to the use of biometric technologies

"Similar sentiments" regarding biometric technologies are also reflected in legal regulation. Although the United States is unique in its structure and has not yet adopted basic federal laws on the use of biometrics, the trends in the practice of individual states can already be seen.

The Illinois Biometric Information Privacy Act (BIPA) was enacted in 2008 as the nation's first state biometric information privacy law. The law requires entities that use and store biometric identifiers to comply with specific requirements and provides a private right of action for recovering statutory damages when they do not. BIPA specifies that "biometrics are unlike other unique identifiers used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." BIPA also states that, for the Act, "'biometric identifier' means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." (Bloomberglaw, 2021)

Texas and Washington also have broad biometric privacy laws, but neither creates a private right of action. Still, other states like Arizona and New York have enacted tailored biometric privacy measures, and many more have enacted a law specifically targeting facial recognition technology (Bloomberglaw, 2021).

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 3 (March)
http://doi.org/10.9770/jesi.2023.10.3(10)

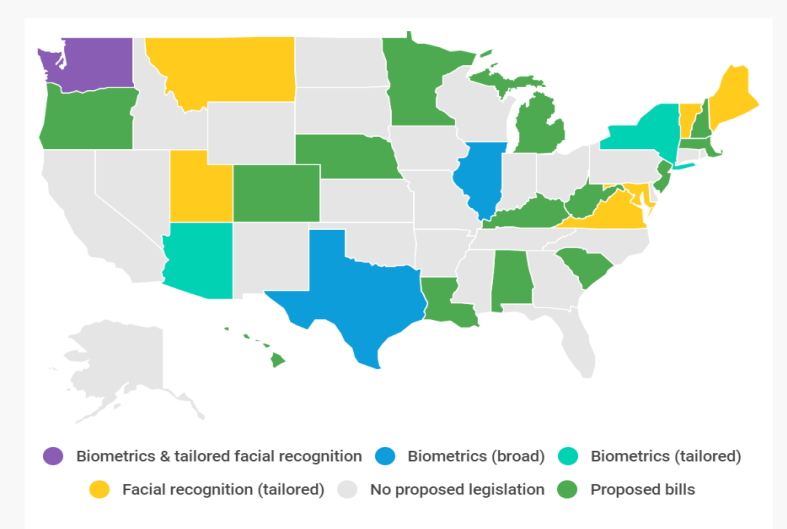

Figure 3. Which other states have biometric privacy laws?
Source: Bloomberglaw, 2021

According to the Privacy Act 1988, (Australian Government, Federal Register of Legislation, n.d.), biometric information is considered sensitive information in Australia. The primary condition for the lawful processing of such personal data is the individual's consent, with some exceptions. Also, data controllers must ensure the highest level of privacy protection in such cases. A person's consent when processing biometric information in the context of employment relations is also possible (provided certain conditions are met). The element of voluntary consent in Australia can be addressed by the employer offering alternative measures for employees to use (Ian Commins, 2021).

The Office of the Australian Information Commissioner, which also oversees the privacy sector, has published general guidelines on the handling of biometric information "Biometric scanning" (OAIC, 2022). According to these guidelines, biometric information scanning is when an organisation or agency takes an electronic copy of your biometric information, which includes any features of your:

- face;
- fingerprints;
- iris;
- palm;
- signature;
- voice.

The guidelines state that an organisation or agency may only scan an individual's biometric information for identification or as part of an automated biometric verification system if the law authorises or requires them to collect it or it is necessary to prevent a serious threat to the life, health or safety of any individual. Hence, Australia seems to be taking a slightly more liberal but controlled path, where the riskiest cases – when a person can be identified using biometric technologies – are only allowed in cases established by law and in certain areas.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 3 (March)
http://doi.org/10.9770/jesi.2023.10.3(10)

In Canada, there are currently no specific legal norms regarding the use of biometric technologies. Data controllers using biometrics are forced to apply general legal norms, which, although technology-neutral, are not considered appropriate for regulating biometrics. This freedom for data controllers to decide on the use of biometrics is deemed not to address the serious risks that arise, especially from the association of biometrics with a specific person. Therefore, additional legal regulation of biometrics is advocated to provide data controllers with clear guidelines regarding in which cases and how to use biometrics (Backman & Kennedy, n.d.). And for now, using biometric technologies in the context of employment relations when processing personal data is permitted in Canada. When an employer decided to use a voiceprint to authenticate employees logging on to a phone system as part of their work, the Privacy Commissioner of Canada said that the use of a voiceprint was legal because the voiceprint could not be used for any other purpose, could not be used to spy on employees, and did not reveal much information about the employee (Privacy Handbook, 2015).

Thus, trends can be seen to regulate individual cases using biometric technologies to identify individuals. In this way, market participants and the data subjects themselves are given greater clarity than leaving situations to be resolved following general data protection legislation.

6 Challenges of using biometric technologies to protect critical information infrastructure

Using biometric technologies that help uniquely authenticate internal employees with access to critical infrastructure for cybersecurity purposes needs to be improved by existing regulations based on the GDPR. The regulation provides general grounds for processing biometric data as a special category of personal data – the processing of these data is subject to a special regime and conditions for lawful processing. Yet at the same time, this means that in protecting critical information infrastructure, these data may only be processed on the basis of the consent of the employee as per GDPR Article 6(1)(a), or if the employee has given explicitly consent as per GDPR Article 9(2)(a). And due to the imbalance between the position of the employer and the employee (imbalance of power (Guidelines 05/2020), such consent is likely to be recognised as not being voluntary unless the employer were to provide alternative systems. However, in the case of giving alternative approaches for the protection of critical infrastructure, it would not be possible to ensure the use of biometric technologies alone for the identification and authentication of infrastructure employees.

The situation could be changed if the EU Member States decided to take legal, regulatory actions establishing a procedure for using biometric technologies in critical infrastructures. In the context of emerging cyber risks and potential harm to society, critical infrastructure could be classified as one of the areas where the use of biometric technologies for employee identification and authentication would be based on GDPR Articles 6(1)(c) and 9(2)(g), i.e. "processing is necessary for reasons of substantial public interest, based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject." (Regulation (EU) 2016/679) This would eliminate those curious situations where, due to the limitations of data protection legislation, the relevant infrastructure managers cannot use biometric technologies in the context of employment relations to protect the infrastructure.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 3 (March)
http://doi.org/10.9770/jesi.2023.10.3(10)

Conclusions

The need to protect critical information infrastructure has always been the most pressing. This need has been exacerbated by Russia's invasion of Ukraine, with countries actively supporting Ukraine facing an even greater risk of cyber-attack since the start of the war. It would be wrong to think that in such cases, only external cyber-attacks need to be guarded against. Internal cyber threats also pose a significant danger and can have even greater negative implications. Biometric technologies can help reduce the risk of internal incidents, as they can uniquely authenticate and identify natural persons – employees, especially since using such technologies in individual sectors is spreading.

However, the association of biometric information with a specific person and the resulting risk in the case of loss or theft make this feature of biometrics a severe threat that requires the use of biometrics for identification to be limited. To that end, specific legislation is already emerging or being put forth for ratification that regulates the use of biometrics when the aim is to identify a person.

In terms of its importance and the risks involved, the area of critical infrastructure and the protection of such infrastructure from cyber threats could be classified as a national priority, and the use of biometric technologies for identification and authentication could be regulated in this area.

In some countries, individual cases where biometric technologies are used for personal processing data are already regulated by legislation. The EU Member States could adopt a harmonised and transparent practice of regulating the use of biometric technologies for cybersecurity so that these technologies could be used by critical infrastructure managers that are currently unable to do so since the consent of the employees may be deemed as not being voluntary. The new practice of legal regulation would allow controllers implementing biometric technologies for identification and authentication to follow GDPR Articles 6(1)(c) and 9(2)(g), i.e. established by legal obligation/national legal regulation, and not risk being penalised by national supervisory authorities for processing excessive data and/or processing a special category of data without the proper legal basis.

The corresponding new practice of national legal regulation classifying critical information infrastructure as an area of national importance where biometric technologies can be used to identify individuals could be coordinated at the EU level by issuing relevant guidelines. Such guidelines could lead to a new wave of legal regulation in individual EU Member States allowing data controllers – critical infrastructure managers – to substantiate their use of biometric technologies for identification and authentication as far as cybersecurity is concerned, i.e. the conditions for lawful processing established in GDPR Article 6(1)(c) and the conditions for lawful processing provided for in GDPR Article 9(2)(g).

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 3 (March)
http://doi.org/10.9770/jesi.2023.10.3(10)

References:

Abuelsamid, S. (2019). Digital voice assistants are the future of in-vehicle control, Automotive World https://www.automotiveworld.com/articles/digital-voice-assistants-are-the-future-of-in-vehicle-control/

Act CCXXII of 2015 on the General Rules for Trust Services and Electronic Transactions, Section 35, https://net.jogtar.hu/jogszabaly?docid=a1500222.tv

Act I of 2004 on the Sport, Sections 72, 72A, 72B, https://net.jogtar.hu/jogszabaly?docid=a0400001.tv

Act I of 2012 on the Labour Code, Section 11, http://www.ommf.gov.hu/letoltes.php?d_id=8133

Act No 483/2001 on Banks and on Amendments to Certain Acts, Section 93a (2), 483/2001 Z.z. - Zákon o bankách a o zmene a doplnen... - SLOV-LEX

Act No 541/2004 on Peaceful Use of Nuclear Energy (the Atomic Act), Section 26 (6) and (7), 541/2004 Z.z. - Zákon o mierovom využívaní jadrovej... - SLOV-LEX

Australian Government, Federal Register of Legislation, n.d. https://www.legislation.gov.au/Series/C2004A03712

Backman, P., & Kennedy, C, n.d. Biometric Identifications and Privacy Concerns: A Canadian Perspective, https://www.airdberlis.com/docs/default-source/articles/biometric-identification-and-privacy-concerns.pdf?s

Baggott, S., & Santos, J. (2020). A Risk Analysis Framework for Cyber Security and Critical Infrastructure Protection of the U.S. Electric Power Grid. *Risk Analysis*, 40(9), 1744-1761. https://doi.org/10.1111/risa.13511. P. 1751

Bloomberglaw. 2021. The Evolution of Biometric Data Privacy Laws. https://pro.bloomberglaw.com/brief/biometric-data-privacy-laws-and-lawsuits/

Cavoukian, A., & Snijder, M.A. (2009). Discussion of Biometrics for Authentication Purposes: The Relevance of Untraceable Biometrics and Biometric Encryption, Information and Privacy Commissioner of Ontario, July 2009 https://doi.org/10.1007/978-3-642-12595-9_3

Chan, H. L., Kuo, P. C., Cheng, C. Y., & Chen, Y. S. (2018). Challenges and future perspectives on electroencephalogram-based biometrics in person recognition. *Frontiers in neuroinformatics*, 12, 66. https://doi.org/10.3389/fninf.2018.00066

Cleary Gottlieb Steen & Hamilton LLP. (2022). Cyber Incident Reporting for Critical Infrastructure Act Signed into Law, 18 March 2022, https://www.clearygottlieb.com/news-and-insights/publication-listing/cyber-incident-reporting-for-critical-infrastructure-act-signed-into-law

Code regarding the protection of personal data, containing provisions for the adaptation of national law to (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, Article 2-septies, https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali+%28Testo+coordinato%29.

Commission for Personal Data Protection, Bulgaria, https://www.cpdp.bg/

Data Protection Commission, 2020 Annual Report, p 25, https://www.dataprotection.ie/sites/default/files/uploads/2021-05/DPC%202020%20Annual%20Report%20%28English%29.pdf.

Dauda, S. Y., & Lee, J. (2015). Technology adoption: A conjoint analysis of consumers′ preference on future online banking services. *Information Systems*, 53, 1-15. https://doi.org/10.1016/j.is.2015.04.006

Economist. (2022). Which countries have pledged the most support to Ukraine?, 2 May 2022 (updated 15 June 2022), https://www.economist.com/graphic-detail/2022/05/02/which-countries-have-pledged-the-most-support-to-ukraine

European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices, 29 January 2020, p 18, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

Global biometric system market revenue in 2020 and 2025, https://www.statista.com/statistics/1048705/worldwide-biometrics-market-revenue/

Global Biometrics Market Report 2021: Market to Reach $44.1 Billion by 2026 - Increasing Significance of Biometrics Technology in Facilitating Contactless Passenger Journey Post-COVID-19 Pandemic, Research and Markets, 11 November 2021. https://doi.org/10.1016/j.fopow.2021.10.039

Guidelines 05/2020 on consent under Regulation 2016/679, European Data Protection Board, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_lt_0.pdf

Healthcare: Global Market Trends for Biometrics. (2020). Global Biometrics in Healthcare Market, Forecast to 2024, https://www.panacearesearch.eu/watch/healthcare-global-market-trends-biometrics

Hernández, A. (2020). Facial recognition in times of pandemic, Mobbeel https://www.mobbeel.com/en/blog/facial-recognition-in-times-of-pandemic/

Ian Commins. (2021). Using Biometrics: What's the status in Australia, Privacy108. https://privacy108.com.au/insights/using-biometrics-in-australia/

i-SCOOP, n.d. Facial recognition 2021 and beyond – trends and market https://www.i-scoop.eu/facial-recognition/

IAPP. (2021). Canadian authorities determine facial recognition firm violated privacy laws, https://iapp.org/news/a/canadian-authorities-determine-facial-recognition-firm-violated-privacy-laws/

Identity verification market revenue from 2017 to 2027. (2022). https://www.statista.com/statistics/1036470/worldwide-identity-verification-market-revenue/

Injunction Order against the Provincial Health Authority of Enna, 14 January 2021, No 9542071, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9542071.

Kindt, E. J. (2018). Having yes, using no? About the new legal regime for biometric data. *Computer Law & Security Review*, 34(3), 523-538. https://doi.org/10.1016/j.clsr.2017.11.004

Kruszka L., Klósak M., & Muzolf, P. (2019). Critical Infrastructure Protection. NATO Science for Peace and Security series https://www.nato.int/cps/en/natohq/topics_168104.htm?

Lithuanian DPA: Fine Imposed on a Sports Club for Infringements of the GDPR in Processing of Fingerprints of the Customers and Employees. EDPB (2021). https://edpb.europa.eu/news/national-news/2021/lithuanian-dpa-fine-imposed-sports-club-infringements-gdpr-processing_en.

LogRhythm. (2022). The state of the Security Team https://logrhythm.com/the-state-of-the-security-team/

Lomas, N. (2021). Clearview AI told it broke Australia's privacy law, ordered to delete data. November 3, 2021. https://techcrunch.com/2021/11/03/clearview-ai-australia-privacy-breach/

Maglaras, L., Janicke, H., & Mohamed, A.F. (2022). Cybersecurity of Critical Infrastructures: Challenges and Solutions. *Sensors*, 22(14), 5105. https://doi.org/10.3390/s22145105

MarketsandMarkets. 2022. Digital Signature Market by Component (Solutions and Services), Solution (Software and Hardware), Deployment Mode, Organization Size, Vertical (BFSI, Government, Healthcare and Life Sciences, Legal, Real Estate), and Region - Global Forecast to 2026 https://www.marketsandmarkets.com/Market-Reports/digital-signature-market-177504698.html?gclid=Cj0KCQjw3v6SBhCsARIsACyrRAmnKS9FjerLH2wwgfS79RwX1bT5WCqAAQmF62H3iw6mPUE_-6kraW0aAsYFEALw_wcB

Meden, B., Rot, P., Terhörst, P., Damer, N., Kuijper, A., Scheirer, W. J., ... & Štruc, V. (2021). Privacy–enhancing face biometrics: A comprehensive survey. *IEEE Transactions on Information Forensics and Security*, 16, 4147-4183. https://doi.org/10.1109/TIFS.2021.3096024

National Cybersecurity Strategy Good Practice, n.d. part 5.4, https://ncsguide.org/the-guide/good-practice/

Noguchi M., & Ueda H. (2021). An Analysis of the Actual Status of Recent Cyberattacks on Critical Infrastructures. *NEC Technical Journal*, 16 https://www.nec.com/en/global/techrep/journal/g17/n02/170204.html

North-Samardzic, A. (2020). Biometric technology and ethics: Beyond security applications. *Journal of Business Ethics*, 167(3), 433-450. https://doi.org/10.1007/s10551-019-04143-6

Office of the Australian Information Commissioner (OAIC), 2022. Biometric scanning https://www.oaic.gov.au/privacy/your-privacy-rights/surveillance-and-monitoring/biometric-scanning

Paganini, P. (2015). Cyber-Attack on Worldwide Nuclear Facilities, Infosec, https://resources.infosecinstitute.com/topic/cyber-attack-on-nuclear-facilities-worldwide-do-not-underestimate-the-risks/

PANACEA, n.d. (Protection and privacy of hospital and health infrastructures with smArt Cyber sEcurity and cyber threat toolkit for data and people), https://www.panacearesearch.eu/

Pascu, L. (2020). Biometric facial recognition hardware present in 90% of smartphones by 2024, Biometric Update, 7 January 2020, https://www.biometricupdate.com/202001/biometric-facial-recognition-hardware-present-in-90-of-smartphones-by-2024

Privacy Handbook, B.C. (2015). Civil Liberties Association https://bccla.org/privacy-handbook/main-menu/privacy5contents/privacy5-13.html

Procedimiento Nº: PS/00010/2021 https://www.aepd.es/es/documento/ps-00010-2021.pdf

Psychology of Passwords: Expanded Digital Lives and Password (Mis)behaviors, LogMeIn, Inc., 2022, https://www.lastpass.com/-/media/9FE0BF5DC473413B8AB4DF3BD8688295.pdf

Quinn, P. (2021). Research under the GDPR – a level playing field for public and private sector research? *Life Sciences, Society & Policy*, 17(1), 1-34. https://doi.org/10.1186/s40504-021-00111-z

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), Article 9(2)(g), https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32016R0679

Relying on vendor mechanisms processing the biometric data for strong customer authentication; Multiple fingerprint samples stored on a mobile device and used for purpose of user authentication, EBA, 2019, https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4651

Report on existing remote on-boarding solutions in the banking sector: Assessment of risks and associated mitigating controls, including interoperability of the remote solutions - December 2019, European Commission Directorate-General for Financial Stability, Financial Services and Capital Markets Union European Commission, https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/report-on-existing-remote-on-boarding-solutions-in-the-banking-sector-december2019_en.pdf

Robb, D. (2022). The Future of Biometrics in the Workplace, SHRM, 22 February 2022, https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/the-future-biometrics-workplace.aspx.

Roshanaei, M. (2021). Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies. *Journal of Computer and Communications*, 9(8). http://doi.org/10.4236/jcc.2021.98006

Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure, Cybersecurity & Infrastructure Security Agency, 20 April 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

Serrano, F., & Kazda, A. (2020). The future of airports post COVID-19. *Journal of Air Transport Management*, 89, 101900. https://doi.org/10.1016/j.jairtraman.2020.101900

Smith, M., & Miller, S. (2022). The ethical application of biometric facial recognition technology. *Ai & Society*, 1-9. https://doi.org/10.1007/s00146-021-01199-9

Statista. (2019). Facial recognition market size worldwide in selected years from 2019 to 2028, https://www.statista.com/statistics/1153970/worldwide-facial-recognition-revenue/

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 3 (March)
http://doi.org/10.9770/jesi.2023.10.3(10)

Statista. (2023). Market share of smartphone fingerprint recognition solutions by technology from 2018 to 2022, https://www.statista.com/statistics/1003600/smartphone-fingerprint-recognition-technology-share/

Statista. (2023). Voice recognition market size worldwide in 2020 and 2026, https://www.statista.com/statistics/1133875/global-voice-recognition-market-size/

Swedish Authority for Privacy Protection 20 August 2019 decision Ref. No DI-2019-2221, https://www.imy.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf.

The National Supervisory Authority for Personal Data Processing. 2018 Annual Activity Report, pp. 15-17, https://www.dataprotection.ro/servlet/ViewDocument?id=1757.

The Office of the Australian Information Commissioner (OAIC), Australian Community Attitudes to Privacy Survey 2020, September 2020. https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/2020-australian-community-attitudes-to-privacy-survey

The Office of the Australian Information Commissioner (OAIC), Clearview AI breached Australians' privacy, 3 November 2021. https://www.oaic.gov.au/updates/news-and-media/clearview-ai-breached-australians-privacy

Tvaronavičienė M., Plėta T., Beretas, C., Lelešienė, L. (2022). Analysis of the critical infrastructure cyber security policy. *Insights into Regional Development*, 04(01), 26–39. https://doi.org/10.9770/IRD.2022.4.1(2). p. 1.

Van Canneyt, T. (2019). The use of biometric data in an employment context https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/the-use-of-biometric-data-in-an-employment-context

Van Natta, M., Chen, P., Herbek, S., Jain, R., Kastelic, N., Katz, E., ... & Vattikonda, N. (2020). The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic. *Journal of Law and the Biosciences*, *7*(1), lsaa038. https://doi.org/10.1093/jlb/lsaa038

Weinberg, A. (2021). Analysis of top 11 cyber attacks on critical infrastructure https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/

Wendehorst, C., & Duller, Y. (2021). Biometric Recognition and Behavioural Detection: Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces, Policy Department for Citizens' Rights and Constitutional Affairs EN Directorate-General for Internal Policies PE 696.968, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf

Zimmerman, H. (2017). The data of you: Regulating private industry's collection of biometric information. *U. Kan. L. Rev.*, 66, 637.

Funding. This article was prepared as part of an awareness raising project Solving Privacy Paradox 2: Promoting High Standards of Data Protection as a Fundamental Right at the Workplace (SolPriPa2WORK). Project partners are personal data protection supervisory authority of the Republic of Lithuania the State Data Protection Inspectorate and Mykolas Romeris University.
This article was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020). The content of this article represents the views of the authors only and are their sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 10 Number 3 (March)
http://doi.org/10.9770/jesi.2023.10.3(10)

Author Contributions: The authors contributed equally; they have read and agreed to the published version of the manuscript.

Darius ŠTITILIS, Faculty of Public Governance and Business at Mykolas Romeris University, Lithuania.
ORCID ID: https://orcid.org/0000-0002-9598-0712

Marius LAURINAITIS, LegalTech center at the Law School at Mykolas Romeris University, Lithuania.
ORCID ID: https://orcid.org/0000-0002-2926-9260

Egidijus VERENIUS Head of Law Division, State Data Protection Inspectorate, Vilnius, Lithuania.
ORCID ID: https://orcid.org/0000-0002-1255-2406