AMERICAN UNIVERSITY OF ARMENIA

ՀԱՅԱՍՏԱՆԻ ԱՄԵՐԻԿՅԱՆ ՀԱՄԱԼՍԱՐԱՆ

LL.M. Program

ԻՐԱՎԱԳԻՏՈՒԹՅԱՆ ՄԱԳԻՍՏՐՈՍԻ ԾՐԱԳԻՐ

TITLE

Characteristics of using biometric data in an employment context: challenges in the Republic of Armenia and possible solutions in the light of international best practice

STUDENT'S NAME

SERGEY SARUKHANYAN

SUPERVISOR'S NAME

LILIT BANDURYAN

NUMBER OF WORDS

10,377

TABLE OF CONTENT

INTRODUCTION

Although biometrics have been used for decades, the technology and new applications have become more prevalent in recent advancements, particularly in the private sector. Biometric technology has become a growingly popular part of daily life. While the use of biometrics is expanding, it exacerbates and exposes individuals and businesses to a range of biometric-related threats and issues. A further impetus for the growth of biometrics is expected to be provided by efforts to establish and implement industry standards. There is a need to attempt to educate people to achieve broader public acceptance. Around the same time, there is a need to examine existing legislative protections concerning the usage of biometric data by the private sector and protect the rights of employees.

Biometrics provides some advantages compared with other authentication systems. The characteristics are well-suited as identifiers because they are unique to each individual. Also, biometric identifiers are convenient; because humans always carry the feature on their body, and it cannot be forgotten, biometrics eliminates the need to remember PINs and passwords or to carry identification documents. However, practice evidenced that there are a lot of questions regarding the security of the individual's data used by the private sector. Biometric systems can be bypassed, compromised, or even failed. A biometric cannot be replaced once exposed, as would a password or other authentication tool. In many cases, employers gather and use biometric data of their employees without even notifying data subject or giving them a clue for what reason their biometric data is being used.

Legislation that will impose barriers to limit the development of biometrics in the private sector is strongly justified. Nowadays, with the development of technical means, many companies started using biometric data of their employees to give them access, to control them, or for other purposes. Mostly, this is done by big corporations to monitor entrance, exit, being in the workplace of their employees. In some cases, biometric data is used to give the employee access to the technology inside the corporation. Even though Armenian legislation practically forbids processing of the biometric data, a lot of companies do so.

Research question: Whether mechanisms of protection of biometric data of employees prescribed by Armenian legislation are effective and are not fictive by their nature? Do these mechanisms serve their aim?

When allowing the employer to use your biometric data, every employee must be aware that a lost password cannot be compared with the stolen biometric data. Biometric data includes part of its subject's identity. Therefore, if stolen, it can do more damage than a stolen password or entrance card. Considering all the above-mentioned Armenian legislation states the following "Biometric personal data is processed … where the purpose pursued by law is possible to implement only through the processing of these biometric data"[1]. We can see that law gives a restriction for using the biometric data and allows usage of the latter when it is the only way to reach the purpose. Despite this, many employers use biometric data of their employees, although they can pursue their goal without using the latter. Hence, we observe a situation when the law prohibits the use of biometric data, but many employers continue to do so. Mentioned is a data minimization requirement, which is embedded both in the Armenian law and the GDPR.

Without comprehensive privacy legislation, we are on the brink of a biometric crisis. The private sector will continue to find new ways to use biometrics, and the security systems that rely on that data will become useless. Therefore, it is wise to be proactive and structure a system of principles and incentives to at least discourage reliance on biometrics.

This paper analyzes the way the private sector, in particular, employers collect and use biometric data of their employees, justifying it in various ways. We will speak about the model of guidelines, approvals, and opportunities to move away from using biometrics by the private sector. We realize that there is no way to entirely avoid the use of biometric data by the private sector. But requiring businesses and individuals to be more careful and strictly reasoned would provide the draftsmen and governments time to understand the threats more deeply, provide better protection, and create security assurance when the system is hacked or fails.

[1] Personal data protection law of the RA

Hence, the structure of this paper will be as follows: chapter 1 introduces the history and drafting of biometrics. Chapter 2 explains the way biometric technology operates, how the private sector collects, and uses biometric data. The third chapter analyzes the general data protection regulation (GDPR). It shows the legal framework for processing of the biometric data in France, Georgia, USA, and in the Republic of Armenia. The discussion suggests that current legal regulations are inadequate to adequately govern the usage of biometric data by the private sector in the Republic of Armenia and to tackle the existing and future possible problems and risks. A set of guidelines on the collection, usage, and storage of biometrics for the private sector are introduced herein. The proposal seeks to create barriers to prevent and (or) justify the use of biometrics by private entities and individuals.

CHAPTER 1. HISTORY AND DRAFTING OF BIOMETRICS

A. International evolution of biometrics usage.

The idea that parts of our body can be used to identify our unique selves is not new. Prints of hand, foot, and finger have already been used in ancient times because of their unique characteristics.[2]

When trying to reveal a specific date for biometrics first usage as a means for identification, it becomes clear that history is not sure on that date. However, what is certain is that since ancient times human beings somehow realized that human characteristics such as the fingerprint were adequate to distinguish him. For example, in Babylon, the fingerprint was being used as a human's signature. Especially with that event, many scholars link the first usage of biometrics by men. Namely, such scholars claim that the early use of biometrics can be dated back to nearly 4000 years ago when the Babylon Empire legislated the use of fingerprints to protect a legal contract against forgery and falsification by having the fingerprints of impressed into the clay tablet on which the contract had been written. [3] This is a manifestation of biometrics' usage – as we call today – by the private sector.

Some sources claim that the first biometrics were evolved in ancient China. In the second century B.C., the Chinese emperor Ts'In She was already authenticating specific seals with a fingerprint.[4] Interestingly, due to that information in fourteenth-century China had presented fingerprinting and had started taking fingerprints of its shippers and their children to differentiate them from all others. Notably, ancient Chinese had found a usage for biometric data in both the private and public sectors.

[2] Els J. Kindt, Privacy and data protection issues of biometric applications, a comparative legal analysis.2013

[3] Richard Jiang, Somaya Al-maadeed, Ahmed Bouridane, Danny Crookes, Azeddine Beghdadi, Biometric Security and Privacy Opportunities &amp; Challenges in The Big Data Era.

[4] https://www.govtech.com/Tracing-the-History-of-Biometrics.html

And in early Egyptian history, traders were differentiated by their physical characteristics.[5]

Biometrics' history was not actively developing from the 15th to 18th centuries. On the contrary, the 19th century is significant for biometric data evolution as such. The potential of fingerprints as a robust identification tool became more famous back then. When working in India in the late 1870's William Hershal noticed the unique characteristic abilities of fingerprints and started using fingerprints as a signature in contracts with Indians.

Then Dr. Henry Faulds was also one of the firsts to see fingerprints as a form of identification, especially for the identification of criminals. He noticed them on old pottery when doing his work in Tokyo, after which he published his thoughts about criminal identification via fingerprints in a scientific journal in 1880.

In the late 19th century, Sir Francis Galton should also get credits for recognizing biometrics as a robust distinguishing tool. He discovered that no two fingerprints were a hundred percent the same, even for twins. He thought that fingerprints remain unchanged and constant during life and might be used as a recognizing tool. Whatsoever, history remains silent on which of the mentioned three men was the first to re-discover fingerprinting as a recognizing tool in the 19th century.

Further, Alphonse Bertillon, a French anthropologist and police desk clerk, developed a method for identifying criminals that became known as Bertillonage.[6] Bertillonage was a measurement system in which estimations of the body are taken for classification and comparison purposes.[7] According to that method, person height, the length of the foot, an arm, and finger had to be taken. Thus, in addition to some body parts measurement, it also required the notions of the body shapes concerning movement, and different unique marks such as scars, birthmarks, etc. However, the time had shown that the measurement of such a nature is not sufficient to identify a person as more than one person with the same measurement occurred as a result. Especially, Bertillon noticed that persons' measurement results did not stay constant and were changing with

[5] Idem.

[6] https://www.globalsecurity.org/security/systems/biometrics-history.htm

[7] Idem

time passing and people growing, and, eventually, it could lead to one person being convicted of another person's crime. It was especially confirmed when in 1903, a person named Will West was confused with another person named William West. Thus, this method of identification disapproved very quickly.[8]

After the failure measurement system, a researcher in Scotland Richard Edward Henry developed the technique of fingerprinting, and it was first implemented in India in 1897. The system assigns each finger a numerical value (starting with the right thumb and ending with the left pinky) and divides fingerprint records into groupings based on pattern types. The system makes it possible to search large numbers of fingerprint records by classifying the prints according to whether they have an "arch," "whorl," or "loop" and the subsequently assigned numerical value.[9] The system started being called as a Henry system. Eventually, it was introduced in England and New York. At the beginning of the 20th century, the New York Civil service started using it in the Army, Navy, and Marines. Thus, it ended up being the most used method of identification in English speaking states.

Fingerprints further were used again by William James Herschel, a British officer in the late 19th and 20th century as a signature for contracts. For the same purposes in 1888 in France, Paris, the Forensic Identification Unit started again using fingerprints. The UK began the usage of fingerprints for person differentiation in 1901.[10]

At the 2001 Super Bowl in Tampa, Fla., face recognition was used to capture an image of each of the 100,000 fans via a security camera and checked electronically against mug shots from the Tampa police. Federal government coordination started in 2003 with the National Science and Technology Council establishing an official subcommittee on biometrics, and a year later, the Department of Defense implemented the Automated Biometric Identification System (ABIS) to help track and identify national security threats.[11]

[8] Idem
[9] Idem
[10] https://www.gemalto.com/govt/inspired/biometrics
[11] https://www.govtech.com/Tracing-the-History-of-Biometrics.html

Hence, we have seen the evolution of usage of the "biometric data" worldwide, which have shown what a long way the biometrics history had to pass to evolve in a specific form we believe in using them today.

B. Directive 95/46/EC and formation of the GDPR

Bearing in mind the events mentioned above, now we would like to turn to the drafting history of biometrics' protection in the European Union. Under article 8 of the European convention on human rights: "Everyone has the right to respect for his private and family life, his home and his correspondence." As we can see, the European Union has worked starting from 1950 to ensure that this right is secured by legislation from this framework.

As a result of the invention of the internet, the growth of the technology, fear by the European Commission that diverging national data protection laws would hinder the internal market in the EU[12], the EU acknowledged the need for new safeguards. In 1995, the European Community adopted Directive 95/46/EC of the European Parliament and of the Council of Oct. 24 1995 on the protection of individuals concerning the processing of personal data and the free movement of such data to harmonize the protection of fundamental rights of individuals with respect to data processing activities and to ensure the free flow of personal data between the EU Member States [13].

While reviewing the provisions of the Directive 95/46/EC, we can see that it does not include any exact clause concerning biometric data. Therefore, the question arises as to whether and when biometric data became personal data, or maybe it is not? Are Biometric Data sensitive personal data? In this regard, it is worth mentioning the article 29 Working Party (hereinafter "Article 29 WP"). This article, under the Directive 95/46/EC, provided the European Commission with independent advice on data protection matters and helped in the development of harmonized policies for data protection in the EU Member States. One of the main tasks of the Article 29 WP is to adopt opinions without a binding character but fundamental to clarify critical

[12] The European Union General Data Protection Regulation: What It Is And What It Means Hoofnagle, C.J.; van der Sloot, B.; Zuiderveen Borgesius, F.

[13] Paul Voigt • Axel von dem Bussche, The EU General Data Protection Regulation (GDPR),A Practical Guide

data protection issues[14]. Hence, we can observe two main elements in the work of the Article 29 WP: first is that it aims to harmonize data protection legislation in the EU states, and second is that it is "soft law," meaning that it has a recommendatory nature.

Having said the above, in its "working document on biometrics," from 2003, article 29 WP tried to analyze and give an answer whether biometric data may be considered as personal data or not. Analyzing the indicated question data protection working party came to the following conclusion: "(…) measures of biometric identification or their digital translation in a template form *in most cases are personal data*. It appears that biometric data can always be considered as "information relating to a natural person" as it concerns data, which provides, by its very nature, information about a given person. In the context of biometrical identification, the person is generally identifiable since the biometric data are used for identification or authentication/verification, at least in the sense that the data subject is distinguished from any other".[15] The Belgian Commission for the Protection of Privacy states that it considers biometric data in principle as being personal data.

Nevertheless, a footnote with this statement mentions that in rare cases, biometric data may not be personal data because a link with persons cannot be established with reasonable means. The commission adds that while data at a given moment in time may not be personal data, they may become later personal data because of new circumstances or new technologies that facilitate identification[16]. So, what we see here is that article 29 WP allows cases when biometric data may be non-personal data because, in its working document, it uses the phrase "in most of the cases." Nevertheless, article 29 WP does not give us a clear understanding regarding cases when biometric data will not be deemed as personal data. The mentioned working document was issued in 2003, and many questions remained unanswered. Also, it is worth mentioning that article 29 WP did not give an exact definition of what is biometric data. It says that: "(…) this kind of data is of a special nature, as it relates to the behavioral and physiological characteristics

[14] Pseudonymization and impacts of Big Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation
Luca Bolognini-Camilla Bistolfi - Computer Law & Security Review - 2017

[15] See: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf

[16] Privacy and data protection issues of biometric applications: a comparative legal analysis
Els Kindt - Springer - 2013

of an individual and may allow his or her unique identification"[17]. From this, we can conclude that article 29 WP deemed biometric data as of special nature and may allow identifying an individual. Definition of the biometric data was later given in the Article 4 (11) of the GDPR as follows: 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data[18]. Here we see that GDPR defines biometric data as personal data.

Speaking about sensitive personal data, Article 29 WP mentions that in addition to the general security measures, additional safeguards shall be provided to such kind of personal data. It also accepts that biometric data, in some cases, can be sensitive personal data. It is said: (…) this does not mean that any processing of biometric data will necessarily include sensitive data[19]. If biometric data is sensitive, then it goes under article 8 of the Directive 95/46/EC, which means that such data shall not be processed. Member states shall prohibit the processing of biometric data. However, article 29 WP does not specify what other biometric data, besides mentioned in article 8, is sensitive data.

But as time went on, the Directive 95/46/EC adopted in 1995 could not manage all the challenges of today. The Directive 95/46/EC started revealing its age and failing to address modern problems related to personal data. Issues, inter alia, included the increase of need for personal data by the public and private sectors, growth of the personal data available online, and of course, processing of biometric data by the private sector (i.e., employers) with the help of modern technologies, which was unavailable back in 1995. Mentioned and a lot of other factors could not be predicted when adopting the Directive 95/46/EC.

Fueled in part by technological and commercial developments since its adoption in 1995, voices in some quarters are increasingly questioning the ability of the Directive to fit for its purpose and are calling for the Directive to be reviewed. These Voices include Institutional Voices (EDPS, UK's Information Commissioner Office (ICO)), and various think-thinks (RAND Europe),

[17] Idem.

[18] Art. 4 GDPR – Definitions, https://gdpr-info.eu/art-4-gdpr/

[19] See: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf

scholars, and experts[20]. The Data Protection Directive did not live up to its objectives and failed to align the level of data protection within the EU. Legal differences arose because of the implementing acts adopted by the various EU Member States.[21]

In 2016, the GDPR was adopted to replace the Data Protection Directive from 1995. It is the result of a robust negotiation process entailing numerous amendments to the legal text that took four years until the adoption of the finalized regulation.[22] Unlike the Directive 95/46/EC, the GDPR applies directly to its addressees — no further implementation steps required by EU member states.

Hence, the protection of the private life of the individual was always an essential issue in the EU. European commission worked hard to ensure the security of the personal data of every individual. For this purpose, Directive95/46/EC was adopted in 1995. Although the directive did not include regulation concerning biometric data, article 29 WP recognized biometric data as personal data in 2003. Moreover, biometric data was thought to be sensitive personal data that needs to have better safeguard than other personal data. GDPR, adopted in 2016, gave a better understanding regarding the essence and terms of processing of biometric data. Regulations provided by the GDPR will be discussed further in this paper.

[20] Data protection law: recent developments, Kasneci, Dede

[21] EU GENERAL DATA PROTECTION REGULATION (GDPR): a practical guide
VOIGT, PAUL. VON DEM BUSSCHE, AXEL - SPRINGER INTERNATIONAL PU - 2018

[22] Idem.

CHAPTER 2 BIOMETRIC DATA IN USE

A. Operation of Biometric system

Previously, we walked through the historical development of the biometrics. With technological development nowadays, both the public and private sectors usually use a biometric system to identify an individual. As mentioned in the introduction, this paper focuses on the private sector.

Biometric characteristics eligible for use in a biometric system for automated comparison shall have specific qualities. The necessary attributes of the characteristics to be used are that the human characteristic shall be universal, persistent, and unique or at least distinctive[23].

As Stephen Hoffman mentioned: "*Biometric systems are pattern recognition systems most often used to verify or identify an individual. A sensor device captures an Individual's biometric characteristic. The device extracts key features from the characteristic and produces a mathematical model called a template. The system predetermines which features it will extract and use for matching, and the templates only encode those extracted features*".[24] Biometric authentication systems generally have one of two uses: to verify an individual's identity or to

[23] Els J. Kindt, Privacy and data protection issues of biometric applications, a comparative legal analysis.2013

[24] Stephen Hoffman, Biometrics, Retinal Scanning, and the Right to Privacy in the 21st Century, 22 SYRACUSE SCI. & TECH. L. REP. 38, 46 (2010).

identify a user based on his biometric credentials[25]. Both verification and identification are used to confirm, recognize the person. An individual presents her characteristic to the device, and the system conducts a search to match the given characteristic against existing templates[26].

The procedure, as mentioned above, briefly described the way how the biometric system works and makes it possible to identify an individual. With the development of technology, the private sector started using biometric systems more often than ever. They implemented biometric recognition systems and collect biometric data of their employees, customers. Hence, the industry is rapidly expanding the prevalence of biometric systems. A lot of corporations justify using biometric data for security purposes. For example, Apple touch ID which allows unlocking the phone by using a fingerprint or face recognition system[27], a lot of banks in Armenia activated usage of fingerprint and face ID for entering into mobile banking applications[28]. Back in October 2014, MasterCard And Zwipe Announced the launch of the world's first biometric contactless payment card with an integrated fingerprint sensor[29] , etc.

From the above mentioned, we can see that the usage of biometric data by the private sector is rapidly growing. The private sector uses biometric data of its employees, clients by giving various reasons. Is there any adequate legal mechanism that governs the technology? One can recover its password in case the system is hacked, but what about the fingerprint, eye, face, etc. As it was correctly mentioned: "biometrics cannot be stored anonymously because they are, by their nature, identifying information[30]."

At first glance, biometrics seems like a win: There's only one you, and unless someone is a modern-day 007 and can somehow perfectly duplicate every ridge, every contour, every detail on your finger, a fingerprint scan is truly a quick and painless way of proving your identity. The

[25] Darcie Sherman, Biometric Technology: The Impact on Privacy, Law Research Institute Research Paper Series CLPE Research Paper No. 5/2005 3 (2005),

[26] Stephen Hoffman, Biometrics, Retinal Scanning, and the Right to Privacy in the 21st Century, 22 SYRACUSE SCI. & TECH. L. REP. 38, 46 (2010).

[27] *Use Touch ID on iPhone and iPad*, APPLE, https://support.apple.com/en-am/HT204587.

[28] See https://www.ameriabank.am/PressContent.aspx?id=6229&subcat=702&mt=image/jpeg&lang=33.

[29] See https://newsroom.mastercard.com/press-releases/thumbs-up-mastercard-unveils-next-generation-biometric-card/

[30] Working Document on Biometrics,12168/02/EN, WP 80, at 5 (Aug. 1, 2003),

issue arises, however, when malicious sources breach biometric data. If a hacker steals your credit card information, Wells Fargo will immediately send you a new card, close the compromised one, and work with you to restore any losses you suffered. In contrast, if a hacker steals your fingerprint scan or your facial recognition data, who do you ask for a new face, a new fingerprint, a different voice pattern? These unanswerable questions are but a few of the driving factors behind the legislation and litigation springing forth from the resurgence of biometric data. [31]

B. Biometric Systems in the Employment Context

An employer always acts as a processor of personal data. It processes personal data even when accepting job applications (for example, personal data of applicants), during work and after dismissal.

Several actors in the private sector are starting to collect biometric data, for example, to secure access to a physical place or particular applications and become controllers of biometric data. These actors include employers imposing biometric access control systems upon their employees and/or contractors, owners of private clubs, school organizations, and banks.[32] Employers are increasingly gathering biometric data from their employees.

Most of the time, employers use biometric data of their employees justifying with the need to control the hours effectuated and the attendance of employees. With this regard, employers shall keep legal requirements regarding the usage of biometric data and ensure the rights of the data subject. Below we will discuss how France deals with the processing of biometric data by the employers.

C. Possible risks associated with traces, forgery, and theft

As it was mentioned, biometric systems have their drawbacks. Once biometric data is exposed, it cannot be replaced, as would a password or other authentication tool. Biometric data is a part of the individual, and it cannot be transferred (or forgotten) in principle. Nowadays, almost every

[31] https://www.bradley.com/insights/publications/2018/05/the-evolution-of-us-biometric-privacy-law

[32] Els J. Kindt, Privacy and data protection issues of biometric applications, a comparative legal analysis.2013

smartphone has face recognition or fingerprint. People use these tools to enter their bank accounts and to use other services.

Article 29 WP mentioned: "(…) some biometric systems are based on information, like fingerprints or DNA samples, that may be collected without the data subject being aware of it since he or she may unknowingly leave traces".[33] One can leave a trace of his/her fingerprint everywhere, for example, in a plate or glass. Those traces can, therefore, be used by interested parties to identify that person or commit fraud, without the knowledge of the individual. One step for avoiding such kind of frauds is to store all the biometric data on servers (technology) held by the personal data protection agency.

Experiments were done in Japan to create artificial fingerprints. They were made by pressing real fingers to the plastic. During the test mentioned, artificial fingerprint systems fooled the fingerprint detectors, about 80 percent of the cases.[34] In Germany, for example, the Computer Chaos Club (CCC) demonstrated the easy access and copying of fingerprint by copying the fingerprint of the Minster of the Interior W. Schäuble from a glass that was used during a speech he gave to protest the use of biometrics data.[35]

One of the well-known cases regarding the hacked system is the case of the *Equifax credit* reporting service. Personal data of over 140 million Americans were hacked[36].

Biometric data is an integral part of a person. It cannot be restored once it is lost. Both public and private sectors must be careful while using such kind of data. Therefore Article 29 WP and now GDPR considered biometric data as sensitive data and included it among the special category personal data, which means that biometric data need to have additional safeguards.

[33] See: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf
[34] Els J. Kindt, Privacy and data protection issues of biometric applications, a comparative legal analysis.2013
[35] Idem.
[36] Ron Lieber, How to protect yourself after the Equifax credit breach

CHAPTER 3. LAW OF THE REPUBLIC OF ARMENIA CONCERNING USAGE OF THE BIOMETRIC DATA, CHALLENGES AND POSSIBLE SOLUTIONS IN THE LIGHT OF INTERNATIONAL BEST PRACTICE

A. Biometric data within the framework of the GDPR

We already discussed the drafting history of the General Data Protection Regulation (the GDPR). In this chapter, we will discuss the legal framework for the processing of biometric data by GDPR, France, Georgia, USA, and the Republic of Armenia.

Article 5 of the GDPR stipulates basic principles that every data processor shall comply with when processing personal data. The mentioned article provides several principles aiming to limit the usage of personal data and allowing the usage when certain legal conditions are met. As was mentioned, biometric data are considered sensitive data, which means that additional and more specific protection shall apply to such data. This is also evidenced by the fact that processing of biometric data was included in Art. 9 GDPR (Processing of special categories of personal data), which generally prohibits the processing of the special categories of personal data. Among other types of data, article 9 also mentions, "biometric data can identify a natural person." It worth mentioning that biometric data was not explicitly provided for as protected categories under the Directive 95/46/EC but have now been included in the GDPR. These categories of personal data require special protection since they require assumptions about an individual linked to his fundamental rights and freedoms, and their processing may present high risks to the latter.

Although, in general, Article 9 of the GDPR prohibits the processing of biometric data, it also provides exceptions in the presence of which biometric data may be processed.[37] In this chapter, we will discuss provided exceptions and will try to understand what GDPR advises to the member states with respect to the processing of the biometric data.

The first exception is the consent explicitly given by the data subject. The data subject may provide its consent for processing his biometric data for a specified purpose. The GDPR foresee that every country's legislation could ensure that the ban on the processing of biometric data cannot be removed with the consent of the data subject. It is doubtful that such a ban would be enforced at the EU level, as the EU has only restricted competences to establish legislation. So, every country must choose for itself whether to limit this right of the data subject or not. Dutch case could be a proper example here. Dutch Supervisory Authority for Data Protection imposed fine in the amount of 725,000 EUR for violating of provisions of Article 9 of the GDPR. The organization had required its staff to have their fingerprints scanned to record attendance. However, as the decision of the data protection authority stated, the organization could not rely on exceptions to the processing of this special category of personal data, and the company could not provide any evidence that the employees had given their consent to this data processing[38]. Mentioned shows the effectiveness of this provision. Another case that shows the importance of explicit consent is the following. A school in Gdansk used biometric fingerprint scanners to authenticate students for the payment process in the school canteen. Although the parents had given their written consent to such data processing, the data protection authority considered the processing of the student data to be unlawful, as the consent to data processing was not given

[37] See: https://gdpr-info.eu/art-9-gdpr/

[38] GDPR Enforcement Tracker
https://www.enforcementtracker.com/, and
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_vingerafdrukken_personeel.pdf

voluntarily[39]. Polish National, Personal Data Protection Office, fined the school in the amount of 4600 EUR.

Second is employment and social security. The processing is necessary for carrying out obligations and exercising specific rights of the controller/data subject *in the field of employment, social security and social protection law* in so far as it is authorized by EU or EU Member State law or a collective agreement according to EU Member State law providing for appropriate safeguards for the fundamental rights and interests of the data subject. This clause determines that employers need to process special categories of personal data, biometric data in our case, in the employment relationship regularly. Nevertheless, the legislation providing for protections must conform to and must be compared to the high degree of data security needed for different categories of personal data.

The third is the protection of the vital interests of the data subject. Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent[40]. All existential needs and interests are vital interests, particularly the protection of life and physical integrity. The incapacity of the data subject does not make their desires meaningless. The presumed will be decisive; if there is the knowledge that the data subject, irrespective of the vital interests at issue, would not have consented to the processing under the given.

Fourth is the processing by non-profit organizations and bodies. The entity's purpose is the only deciding element to fall under this clause, whereas its legal type or structure is irrelevant. Given such organizations' purposes, their operation typically depends on some legal authorization to process confidential personal data. And of course, these personal data cannot be released outside the organization without the data subject's consent.

The fifth is the personal data manifestly made public by the data subject. In this case, we are talking about the data that was made public with the decision of the data subject (for example,

[39] Idem
[40] Art. 9 GDPR – Processing of special categories of personal data
https://gdpr-info.eu/art-9-gdpr/

data that is published on Facebook, other public websites). However, it is hard to make public biometric data such as fingerprints or iris.

Sixth is the establishment of legal claims. In this scenario, the processing of sensitive personal data during the legal proceedings is necessary for proof. In this respect, the right to privacy of the data subject is outweighed by the requirement of processing the data of the data subject to provide evidence during the litigation. For example, a former employee of the organization sues the organization for dismissing him. The organization uses records of the fingerprints of the employee to prove that the employee was always late from work.

Seventh are reasons of substantial public interest. The processing is necessary for reasons of substantial public interest and takes place based on EU or EU Member State law. These regulations must be proportionate and allow for sufficient data privacy protections. Since there is a need for significant interest, such interest would have to meet high demands as to its value. Fundamental rights, as well as maintaining the life of a society, or the lives, safety, and freedom of individuals, will fulfill that.

Health care is the next exception. Processing is necessary for preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services based on Union or Member State law or according to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3[41]. Where the processing is done based on such a contract, it must be carried out by or under the supervision of a practitioner subject to the obligation of practitioner confidentiality under EU or Member State law (such as a doctor), Art. 9 Sec. 3 GDPR. It will improve data security in situations where the collection is not based on laws as regards confidential personal data.

The Office of the Commissioner for Personal Data Protection of Cyprus announced, on Jan. 13, 2020, its decision to fine the Louis Company Group 82,000 EUR for violating Articles 6(1) and 9(2) of the GDPR. In particular, the decision noted that the use of the Bradford Factor for

[41] Idem.

employee profiling and sick leave monitoring constituted unlawful processing of personal data and, thus, had violated Article 6(1) of the GDPR. Besides, the Commissioner highlighted that dates and information on employees' sick leave are considered as special categories of personal data under Article 9(1) of the GDPR.[42]

The remaining exceptions include public health and research reasons.

As we can see, Article 9 (2) of the GDPR gives several exceptions when sensitive data (i.e., biometric data) can be processed. Understandably, all states have their unique legal systems, and it is impossible to foresee all the possible scenarios for all states. Hence, Article 9 (4) provides for the possibility for the EU Member States to maintain or introduce further conditions regarding the processing of biometric data. This means that during the process of implementation of the GDPR, every state may include further limitations regarding the processing of biometric data in their legislation, which was evidenced by the above-mentioned mentioned cases. Hence, we can see that GDPR ranks biometric data among sensitive data which require additional measures of safeguards in comparison with other category personal data.

The Legal Framework for the Processing of Biometric Data in France

As we analyzed, GDPR allowed and suggested Member states regulate cases, when exactly biometric data can be processed in their country. Guided by the GDPR, France's data protection authority, the CNIL has adopted a regulation setting down legally binding guidelines for data controllers subject to French law who use biometric systems to track access to workplace premises, computers, and applications. The regulation prescribes specific requirements for the processing, by a public or private employer, of biometric data to control accesses to work premises, to information systems or applications used in the context of business tasks entrusted to data subjects (i.e., employees, agents, interns, and contractors)[43].

[42] Cyprus: Commissioner fines Louis Company Group for GDPR violation https://www.dataguidance.com/news/cyprus-commissioner-fines-louis-company-group-gdpr-violation

[43] FRANCE: THE FIRST CNIL STANDARD REGULATION FOR BIOMETRIC SYSTEMS IN THE WORKPLACE Alexandrebalducci - https://blogs.dlapiper.com/privacymatters/france-the-first-cnil-standard-regulation-for-biometric-systems-in-the-workplace/

The regulation considers biometric data as sensitive data and, thus, puts strict conditions for processing such data in the workplace. The regulation sets the following requirements:

- ✔ *The employer shall justify the use of biometrics:* The employer shall demonstrate that the company cannot reach its aims by means other than the processing of biometric data. Given the background at hand, the data controller must document why such a high degree of protection is required and show that biometric data processing is the most important means to ensure security. What regulation says is that the employer must provide documents justifying the need for biometric data and show data controller why other authentication methods like passwords, passcards cannot work in this particular case.
- ✔ *Restrictions:* only biometric authentication based on morphological characteristics of data subjects may be used, and the biometric mean selected (e.g., use of iris recognition rather than fingerprints) must be documented and justified. Biometric authentication based on biological sampling (e.g., saliva or blood) is prohibited for the Regulation[44]. Here we can see that the regulation divides various types of biometric data and, while allowing to process one type, prevents processing of the other.
- ✔ The Model Regulation also stipulates maximum retention periods for biometric data. For example, raw biometric data (such as a photo or audio recording) cannot be retained any longer than necessary to create a biometric template that can be analyzed by the system's software. Moreover, any resulting biometric templates must be encrypted and eventually deleted once an employee no longer works at the organization. The Model Regulation also outlines the types of individual personal data that may reside on a biometric control device and the types of log data that may be collected[45].

French data protection authority took into account that unlike other personal data, biometric data (such as a person's face or fingerprints) is permanent and cannot be altered to prevent abuse if stolen or otherwise compromised. Bearing this in mind, CNIL provided a regulation that will

[44] Idem.

[45] French DPA Issues Robust Model Regulation for Biometric Access Controls in the Workplace https://privacylaw.proskauer.com/2019/04/articles/gdpr/french-dpa-issues-robust-model-regulation-for-biometric-access-controls-in-the-workplace/

ensure and secure processing of the biometric data in the employment context. Therefore, the CNIL provided for strict and clear rules that will govern this sphere. Inter alia, the rules include clear justification (with proper documents) of the purposes of the processing of personal data of the employees by the employer, restriction to use some types of biometric data notwithstanding the consent from the data subject.

We can see the strict regulations by observing the following case. CNIL fined “ASSISTANCE CENTER d'APPELS” in the amount of 10,000 euros for violating terms of usage of the biometric data of the employees in the workplace[46]. During an audit at the end of 2016, CNIL found that the company was using fingerprint timeclocks to track employee hours without prior authorization from CNIL as required[47]. CNIL made its decision public to remind employees of their rights and employer of their obligations with respect to the processing of biometric data in the workplace[48].

Analyzing those mentioned above, we can see how France deals with the usage of biometric data by the private sector. CNIL imposed strict regulations regarding the processing of biometric data in the workplace and conducted investigations and inspections to identify violators. France's example clearly shows what mechanisms can be used when dealing with the biometric data processing issue.

The Legal Framework for the Processing of Biometric Data in Georgia

The main instrument regulating the relations connected with the personal data processing in Georgia is the law of Georgia "On Personal Data Protection." Article 2(c) gives the definition of the biometric data, which is quite like the definition given in the law of the Republic of Armenia. Piques interest how Georgian legislator divides usage of biometric data by public and private sector. Under the Article 10 of the personal data protection law of Georgia, a legal entity under private law and a natural person may only process biometric data if it is necessary to perform

[46] https://www.cnil.fr/fr/biometrie-au-travail-illegale-sanction-de-10000-euros

[47] Shanna Pearce - https://www.mondaq.com/france/data-protection/746262/france-imposes-fine-for-unauthorized-use-of-fingerprint-timeclocks

[48] Idem

activities, provide human safety and property protection, also to prevent disclosure of secret information, if these goals may not be reached by other means or require unjustifiably high efforts. Unless otherwise determined by law, before using biometric data, a data processor shall provide the personal data protection inspector with the same information that is provided to the data subject, in particular on the purpose of data processing and the security measures taken to protect the data[49].

Analyzing the provision of Article 10, we come to the following conclusion. As a rule, Georgian legislator prohibits the usage of the biometric data, as GDPR does, by the private sector unless one of three conditions is present, provided that the goal may be reached only by using biometric data or does not need unjustifiably high efforts. We, therefore, conclude that the processing of personal data may be allowed under the law for the purposes above as an exception provided that the achievement of the purpose by other means requires unjustifiably high efforts.

So, we can see that Georgian legislator gives three criteria as an exception and allows the usage of biometric data if one of the mentioned criteria is present. Hence, as we will see below, both Armenian and Georgian laws provide broad definitions regarding using biometric data, which may be interpreted in different ways. However, Georgian law provides for better security, as it, in general, prohibits the usage of biometric data except for the three mentioned situations.

The Legal Framework for the Processing of Biometric Data in the USA

USA's government has been carrying out biometric data-collecting initiatives for longer than most citizens might realize, for example, the FBI began its national fingerprint collection in 1924.[50]

The Privacy Act of 1974 is the primary legislation governing the federal collection, use, and disclosure of personally identifiable information. The statute falls short, however, of providing for robust protection of the types of technologies that mark the biometrics realm. Reporting requirements, for instance, are limited to data associated with specific individuals. The act only

[49] Idem.

[50] Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data, Carra Pope

applies to federal entities, not state and local governments. And only U.S. citizens and permanent residents fall within the legislation's requirements.[51]

States try to organize the situation regarding the use of biometric data by restricting the collection and use of biometrics. New York generally prohibits fingerprinting as a condition of employment[52]. Two states, Illinois and Texas, have passed laws that specifically apply to the private sector's collection and use of biometrics. Both state laws require an individual to be notified and consent to the collection and restrict the collector's ability to sell, lease, trade, or disclose the biometric without the individual's further consent. Illinois also requires that a collector create a written policy with retention guidelines whereby the biometric is destroyed once the initial purpose has been satisfied or within three years of the individual's last contact with the collector. Texas does not explicitly state any retention requirements beyond storage with reasonable care. Finally, both laws provide remedies for violations of the statute: Texas imposes a civil penalty, while Illinois creates a private right of action for affected individuals.[53]

Washington has passed its laws regulating the use of biometrics in 2017. The Washington statute is explicitly aimed at companies that collect and market biometric data without users' knowledge. [54]

These were the examples of how states in the USA try to secure an individual's biometric data. We see that not all the states pass laws regarding the restriction of using biometric data of employees like it was done in New York. Another question is whether these laws are enforced and valid in New York.

In a perfect world, the anticipation of biometrics usage would be the best way to anticipate the commodification of biometrics. Fingers, eyes, confrontations, voice, and other traits constitute a personal value of humans. The use of biometrics by the private sector, for different purposes, monetizes the characteristics. The latest rise of biometrics usage has driven to the commodification of persons' characteristics, and the usage of modern technology has even raised

[51] Laura K. Donohue, Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric *Identification Comes of Age*, 97 MINN. L. REV. 407 (2012).

[52] N.Y. LAB. LAW § 201-a (McKinney 2014).

[53] 2015 Biometric Boom: How the Private Sector Commodifies Human, Characteristics, Elizabeth M. Walker

[54] Washington's New Biometric Privacy Law: What Businesses Need to Know, VI &. REMINE LLP July 2 , 2017

dangers. A framework of defaults, disclosures, and taxes will not forbid the usage of personal information. Still, it will try to prevent organizations and people from setting up and using such frameworks. The main aim is to buy time in biometrics usage until new proper measures of protection of personal information will be put in place.

The Legal Framework for the Processing of Biometric Data in the Republic of Armenia

After analyzing the GDPR and different legal systems concerning biometric data usage, we will now speak about the Armenian legislation and compare it to the ones mentioned above. In Armenia as well with technological development, biometrics became more prevalent, especially in the private sector with technical progress.

Following the provisions of the article 34 of the Constitution of the Republic of Armenia, *everyone shall have the right to protection of data concerning him or her, details related to the protection of personal data shall be prescribed by law*. As we see, the Constitution of the Republic of Armenia ensures personal data protection. The new law on "Personal data protection" (hereinafter in this Chapter: the Law), adopted on May 18 2015, regulates *inter alia* procedure of usage of the biometric data by data processors (for example employers) their rights, and obligations while working with biometric data and data subjects. When comparing the old law of the Republic of Armenia on "Individual data" with the Law, it must be noted that the former did not include any mentioning of biometric data. At the same time, the Law not only defines that phenomenon but also puts certain procedural obligations on the organizations when processing biometric data[55]. General requirements related to the processing of employees' data by the organizations can also be found in the "Labor Code" of the Republic of Armenia. The Labor code gives general requirements but refers to the Law for specific cases. Analysis of the Law will give us answers about the effectiveness of the latter.

Article 3(1)(13) of the Law describes biometric data as follows: "*biometric personal data" shall mean information characterizing the physical, physiological, and biological characteristics of a person."* Article 13 of the Law stipulates that "*personal biometric data shall be processed only*

[55] The Law of the Republic of Armenia on “Individual data” lost its legal force when the Law on “Personal data protection” adopted on 18th of May 2015.

by the data subject's consent ... and where the purpose pursued by law is possible to implement only through the processing of these biometric data". Following Article 23(3), "*the processor, before the processing of biometric or special category personal data, shall be obliged to notify the authorized body for the protection of personal data of the intention to process data."*

Analyzing the previous, it becomes clear that Armenian legislator requires the processor of biometric data to satisfy the following requirements before processing:

- have the written consent of the data subject,
- notify personal data protection agency (hereinafter: the "Agency") about the intention to process biometric data,
- the set goal can only be achieved by using biometric data.

The first step before processing any personal data is getting consent from the data subject. GDPR has the same provision. Armenian legislation has enough adjustment concerning the way of notification and getting consent from the data subject. Article 9 of the Law gives the mentioned regulation under which to get the written consent of the data subject; the processor is obliged to notify the data subject about his intention to process the data subject's data and also the purpose of the processing, which is mandatory. Data Subject should be informed in a clear and understandable form about the conditions, goals, and purposes of use of his data.

The second is to notify the Agency. Under Article 23 of the Law, *the processor has the right to notify the Agency before processing of personal data*. The case is different when it comes to biometric data. The Law *obliges* the processor to notify the Agency before processing of biometric data.

The third is the purpose for which the personal biometric data shall be used. Biometric personal data are such physical, physiological, and behavioral characteristics of a person that are unique, consistent, and specific to a person. Physical symptoms include human fingerprints, rainbow eyelids, facial features, the structure of the hand and foot, and much more. Technical equipment and electronic systems are sometimes installed to collect biometric data to control people's access to state and private institutions. The equipment processing biometric data shall be installed only when there is no other way to achieve the purpose.

It is clear that under Armenian legislation, it is allowed to use biometric data only in limited cases, as almost every goal can be achieved without using biometric data. For example, the employer uses fingerprints to identify employees and monitor their arrival at work. But can't employers do this without using fingerprints? They can. The employer can use passcards so that every employee will check at the entrance and exit to the building. Does the employee have the right to refuse to provide his biometric data to the employer?

Under the provisions of the Law, the employee has the right to receive complete information about his biometric data and their processing (Article 15 of the Law). In particular, the employer must provide information on the basics and purposes of data processing, as well as on the circle of persons who has access and to whom biometric data can be transferred. The employer must provide or enable information about the processing of the employee's biometric data within five days of receiving their written request. The employee has the right to require the employer to delete or destroy his / her biometric data if they have been obtained illegally (the legal basis is absent) or are not necessary for processing.

We can see that the employee has the right not to let the employer use his/her biometric data. In most cases, employees are not aware of their rights. Also, employers do not give them the right to choose, saying that one can become their employee only by giving consent to use his/her biometric data. Thus, the solution to the problem should be approached not by exercising the rights of the employee, but by limiting the rights of the employer. Strictly speaking, the legislator must restrict usage of the biometric data by the employers or at least put several limitations and requirements as the French data protection authority did. Thus, the right of an employee to reject the provision of his/her data is just a fiction; it becomes mandatory to get the job they applied for (note that we are discussing the personal data in general, as the employer needs to have a name, passport, etc. of the employee to register the latter as an employee.). It seems that the regulation provided for by the Law does not adequately serve its purposes. By saying, "the purpose pursued by law is possible to implement only through the processing of biometric data," the Law gives too broad concept regarding allowing or prohibiting the use of biometric data. If the legislator wanted to ban the use of biometric data completely, then what is the point of giving such a broad concept for use?

When we compare GDPR with the Law, we observe the following differences:

- GDPR included biometric data in the section of the special category personal data defining them as sensitive data, which means that biometric data need to have additional safeguards. Armenian legislators did not include biometric data in any category of personal data and stipulated biometric data separately.
- GDPR stipulates ten exceptions when the usage of biometric data can be allowed. Armenian legislator does not bring any exceptions or cases when the usage of biometric data can be approved. Instead of this, the Armenian legislator gives a broad interpretation stating that "the purpose pursued by law is possible to implement only through the processing of biometric data."

It is crucial to consider the technical progress all over the world and the fact that the prohibition of usage of biometric data will not be the best solution for the problem. Instead of prohibiting or giving the broad interpretation, Armenian legislators can use the example of GDPR, France, and stipulate several exceptions, when the usage of biometric data is allowed. By making the mentioned mechanisms Agency will control the usage of the biometric data much more effectively.

B. Possible solutions considering international best practices.

As we talked in the previous chapters, states shall ensure better protection of sensitive data of its citizens and take appropriate and reasonable measures for implementing the said. Article 9 (4) of the GDPR also mentioned the need to provide better protection to the biometric data. For this purpose, states adopt normative legal acts that protect the constitutional rights of citizens. In comparison with other countries, the development of personal data protection in the Republic of Armenia took longer. In recent years, the private sector in the Republic of Armenia started using biometric data of their employees more often. This means that additional biometric data protection rules (regulations) shall be implemented to minimize the usage of biometric data by the private sector. As it was mentioned several times in this paper, the loss of the password or passcard is noncomparable with the lost biometric data.

In this paper, we reviewed the legislation of different states concerning biometric data and tried to compare them with the "Personal data protection" law of the Republic of Armenia. Hence, there are several things that our legislator could change or add to regulate better the usage of biometric data by the private sector. The loss of biometric data may be irreversible. History knows several cases when biometric data was breached or hacked by malicious sources. The government shall control this. Ideally, the best way of preventing usage of the biometric data by the employers is to prohibit the use of the latter at all. But it will not be valid, as an especially big corporation that has many employees need biometric data to monitor employees, to give them access, etc. Thus, mechanisms shall be implemented to limit the usage of the biometric data and control, biometric data processors.

In the guide prepared by the Agency, they gave recommendations concerning usage of the biometric data by the employers to regulate being in the workplace of their employees. The point was that the employer should not use the fingerprint of the employee to monitor the entrance and exit from the workplace[56]. Employers do not comply with this guide because it is only advisory. The legislator cannot stipulate every single case in the Law, and it will not be efficient to prohibit the usage of the biometric data at all. In this case, the Armenian legislator may stipulate the instances when it is forbidden to use the biometric data or put the strict requirement for processing.

We would suggest stipulating usage of the biometric data by the private and public sectors in different articles of the Law as the first step. This will allow mentioning the situations when governmental agencies can use the biometric data of the citizens. In this case, we can say for sure that the government has full control over the public agencies. This also will allow minimizing or limiting usage of the biometric data by the private sector.

[56] GUIDE ON PERSONAL DATA PROTECTION IN LABOR RELATIONS, Yerevan 2017. Available at http://www.justice.am/storage/uploads/002employee_guide-10.04.2017.pdf

The second step aimed at minimizing the usage of biometric data is the adoption of the robust requirements for the processing of biometric data in the workplace by the employer. Analyzing the international practice in this paper, we can say that the Republic of Armenia may use the France approach for regulating the usage of biometric data by the private sector. For this purpose, several criteria shall be implemented in the Law in the presence of which data subject's consent will not be enough to process biometric data. Those criteria will be discussed below.

Justification: the data processor must document why such a high degree of protection is required and show that biometric data processing is the most important means to ensure security (including the basis for selecting one biometric feature over another for authentication). The following case shows the hard side of justifying the processing of biometric data. Data protection authority of Sweden fined a school for using facial recognition technology that was used for monitoring student's attendance. The authority found that the mentioned purpose could be achieved without using facial recognition technology[57].

Data Minimization: the private sector may use only a limited category of biometric data. A list of the prohibited biometric data shall be provided (for example, biometric authentication based on biological sampling, etc.). In this instance, it would be appropriate to mention the fine imposed on Entirely Shipping & Trading S.R.L. on 13.12. 2019 by the Romanian data protection authority. The company processed biometric data (fingerprints) of the employees for access to certain rooms tough less intrusive means for the privacy of the data subjects could be used (violation of the principle of "data minimization")[58].

One centralized database for storage of biometric data: in case the processor justifies the need for the processing of biometric data, this data will be stored in a database to which the government shall have access for controlling it.

[57] See:
https://www.datainspektionen.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf

[58] GDPR Enforcement Tracker
https://www.enforcementtracker.com/

Biometric data is sensitive personal data, which means that governments shall impose strict regulations concerning the processing of biometric data. As we mentioned, the current wording of the Law (personal data protection law of the RA) is not precise, and one can give a different perception of the provisions regarding the processing of biometric data. The Law needs to be more specific. Mentioned implementations will make the Personal data protection law of the Republic of Armenia much more effective. Agency will have more power controlling the processing of biometric data by the private sector.

CONCLUSION

Biometrics is increasingly entering everyday life, with the aid of technological advancements and the participation of the private sector. Fingers are more than just body parts; they are keys to an account. Faces and voices are no longer only exchanged with neighboring people but are value-added products tradable to businesses. The exponential development of biometrics transforms into something that can be traded and sold until non-monetized attributes are something. This commodification, in effect, highlights the shortcomings of biometric technology, which only gets amplified as more systems are introduced. There are inherent security vulnerabilities in biometric systems, and hackers will still knock at the door. Those wanting to use biometrics for safety purposes simply turn over identities to hackers and leave people with unique identifiers.

Without comprehensive privacy legislation, we may be on the brink of a biometric crisis. The usage of biometric by the private sector is just gaining momentum in the Republic of Armenia. The government can limit, minimize the risks that may arise in the future by amending existing legislation, and by turning it against the employers that use biometric data of their employees not thinking about the possible risks. The private sector will continue to find new ways to use biometrics, and the existing legislation will become useless. It is, therefore, prudent to be cautious and to develop a program of values and rewards to deter at least dependency on biometrics. Through this paper, the proposed set of principles and methods would create barriers in the race to implement biometrics. Essentially, when technology fails, people, businesses, and the legal system need to be more educated and prepared.

In this paper, we analyzed the legal systems of France, the USA, Georgia. We analyzed GDPR adopted in 2016 and compared them with the Armenian personal data protection legislation. We observe that GDPR, France, and Georgia accept biometric data as sensitive personal data and include them in a special category of personal data. In contrast, Armenian legislators did not include biometric data in the special category of personal data. While Armenian legislators gave broad, not precise wording to the processing of biometric data (the purpose pursued by law is possible to implement only through the processing of biometric data), France marked clear boundaries as to when the usage of biometric data is not prohibited.

In the light of the international best practice and considering the technological progress in the world, better regulation concerning the processing of biometric data shall be implemented in the personal data protection law of the Republic of Armenia. It is the clear differentiation between private and public sectors, having one centralized database, justification of the processing of personal data in front of the Agency by providing documents and data minimization.

BIBLIOGRAPHY

Publications.

1. Els J. Kindt, Privacy and data protection issues of biometric applications, a comparative legal analysis.2013

2. Richard Jiang, Somaya Al-maadeed, Ahmed Bouridane, Danny Crookes, Azeddine Beghdadi, Biometric Security and Privacy Opportunities &amp; Challenges in The Big Data Era.

3. The European Union General Data Protection Regulation: What It Is And What It Means Hoofnagle, C.J.; van der Sloot, B.; Zuiderveen Borgesius, F.

4. Paul Voigt • Axel von dem Bussche, The EU General Data Protection Regulation (GDPR),A Practical Guide

5. Pseudonymization and impacts of Big Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. Luca Bolognini-Camilla Bistolfi - Computer Law & Security Review – 2017

6. Data protection law: recent developments, Kasneci, Dede

7. Stephen Hoffman, Biometrics, Retinal Scanning, and the Right to Privacy in the 21st Century, 22 SYRACUSE SCI. & TECH. L. REP. 38, 46, (2010).

8. Darcie Sherman, Biometric Technology: The Impact on Privacy, Law Research Institute Research Paper Series CLPE Research Paper No. 5/2005 3 (2005),

9. FRANCE: THE FIRST CNIL STANDARD REGULATION FOR BIOMETRIC SYSTEMS IN THE WORKPLACE Alexandre Balducci.

10. Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data, Carra Pope.

11. Laura K. Donohue, Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric. Identification Comes of Age, 97 MINN. L. REV. 407, (2012).

12. 2015 Biometric Boom: How the Private Sector Commodifies Human, Characteristics, Elizabeth M. Walker

Legal Documents.

1. Personal data protection law of the RA.

2. Personal data protection law of Georgia.

3. General Data Protection Regulation (GDPR).

4. Directive 95/46/EC of the European Parliament and of the Council of Oct. 24 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

5. Working Document on Biometrics,12168/02/EN, WP 80, at 5 (Aug. 1, 2003).

6. France: The First CNIL Standard Regulation for Biometric Systems in The Workplace.

Web sources

1. Tracing the History of Biometrics
https://www.govtech.com/Tracing-the-History-of-Biometrics.html

2. Biometrics: authentication & identification (definition, trends, use cases, laws and latest news) - 2020 review
https://www.thalesgroup.com/en/markets/digital-identity-and
security/government/inspired/biometrics

3. Use Touch ID on iPhone and iPad

https://support.apple.com/en-am/HT201371

4.https://www.ameriabank.am/PressContent.aspx?id=6229&subcat=702&mt=image%2Fjpeg&lang=33

5. Thumbs Up: Mastercard Unveils Next Generation Biometric Card

https://newsroom.mastercard.com/press-releases/thumbs-up-mastercard-unveils-next-generation-biometric-card/

6. Sensitive to the Touch: The Evolution of U.S. Biometric Privacy Law

https://www.bradley.com/insights/publications/2018/05/the-evolution-of-us-biometric-privacy-law

7. GDPR Enforcement Tracker

https://www.enforcementtracker.com/

8. Cyprus: Commissioner fines Louis Company Group for GDPR violation

https://www.dataguidance.com/news/cyprus-commissioner-fines-louis-company-group-gdpr-violation

9. France Imposes Fine For Unauthorized Use Of Fingerprint Timeclocks - Privacy - France

Shanna Pearce - https://www.mondaq.com/france/data-protection/746262/france-imposes-fine-for-unauthorized-use-of-fingerprint-timeclocks

10. GUIDE ON PERSONAL DATA PROTECTION IN LABOR RELATIONS, Yerevan 2017. Available at http://www.justice.am/storage/uploads/002employee_guide-10.04.2017.pdf

11. https://www.datainspektionen.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf