Journal of Engineering Science and Technology Review
Special Issue on Telecommunications, Informatics, Energy and Management 2019

JOURNAL OF
Engineering Science and Technology Review

Conference Article

www.jestr.org

Government Possibilities to Compel the Use of Body Parts to Unlock Phones and Other Devises

Anastassia Dyulgerova

University of Telecommunication and Post, Department of Basic Training, Sofia, Bulgaria

Received 25 September 2019; Accepted 18 February 2020

Abstract

The biometrics and biometric data were always a delicate issue. Undoubtedly, their security has been addressed many times in legal, social and economic terms. However, other issues remain in the background. This large set of questions concerns the capture and use of biometric data by governments. This work covers only a small part of these issues - the right of governments to compel the use of biometric data to unlock phones and other devices. The article addresses this issue, not because other human rights questions about biometrics are not important, but because of the authorities' repeated attempts to force individual citizens to give them access to their devices by using that data. This has led to a newly established case law and a different view of biometric data.
The current research addresses two main aspects: 1. Do governments may make such requests and force then on the citizens, and 2. Do those requests are just a breach of rights or, by its very nature, a greater violation, such as the violation of constitutionally recognized rights and rights as recognized by the Universal Declaration of Human Rights.
The article starts with defining the main concepts of biometric and how they compel to the usage of body parts to unlock devises. It gives the main legal aspects of biometrics and the aspects of collision of the police compel the use of body parts to unlock phones and other devises and the human rights. Attention is also paid to the analysis of the Bulgarian legislation, the EU legislation, some international acts and the few court decisions on the issue.

Keywords: biometric, smartphones and other devises, devises unlocked by body parts, human rights, education

1. Introduction

The biometrics is subject to the modern acts and bills developing nowadays all around the world. Legislators and courts are trying to define its scope in order data privacy and human rights to be protected. On other hand governments have the difficult task without violating the data privacy and the human rights to protect their citizens from the many crimes committed through technology. This is one of the major collisions that arise within the use of biometric data. Where does the rule of law extend, and where is the boundary between human rights and crime prevention?

2. Some words on biometrics and law

2.1 What the Law understands as biometrics

"Biometrics" or "biometric authentication" typically refers to automated methods for identifying or recognizing an individual based on one or more unique characteristics [1]. Common and developing types of biometrics are: fingerprints, palm prints, iris or retinal scans, facial geography, gait analysis, voice ID, etc.

Biometric information means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual under the Illinois Biometric Information Privacy Act (BIPA) [2]. BIPA was passed by the Illinois General Assembly on October 3, 2008 to guard against the unlawful collection and storing of biometric information. Pursuant to the act biometric identifier means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. This means that writing samples or signatures, photographs, physical descriptions such as height, weight, hair color, or eye color, information captured from a patient in a health care setting and demographic data are not included. Those are covered by the data privacy acts.

One of the latest breakthrough cybersecurity technology is the behavioral biometrics. The lather authentication/verification and identification procedures are based on how the human interacts with the device, such as gait analysis, mouse use characteristics, keyboard pressure, hand tremors, navigation, scrolling and other finger movements, etc.

Paragraph 1 (16) of the Additional Provisions of the Bulgarian Personal Documents Act states that "Biometric Data" is the image of the citizen's face and his fingerprints, which are used for identification and verification of the requested identity. Using of biometric data is undoubtedly personal data as defined by the legislator in Article 2, paragraph 1 of the Protection of Personal Data Act.

The most common contexts for use of biometrics from a governmental point of view are: criminal investigation,

* E-mail address: anastassia_dyulgerova@abv.bg
ISSN: 1791-2377 © 2020 School of Science, IHU.
All rights reserved.

border screening, intelligence surveillance, combat identification, physical access control and device access control. Biometric are used in the commercial field for: device access control, identity verification for transactions, identify verification for human resources, physical access control and targeted advertising.

Biometric data processing is now often used in automated authentication/verification and identification procedures, in particular for the control of entry to both physical and virtual areas (i.e. access to particular electronic systems or services) (12168/02/EN, WP 80).

The two main functionalities of biometrics which differ in purpose and in the way of function are: the verification function and the identification function.

2.2 The legal principles in the use of biometrics

Bulgarian and EU law are focused mostly on biometric applications for verification, e.g. for access control purposes (authentication/verification).

One of the basic EU documents on biometrics is Opinion 3/2012 on the development of biometric technologies of the Article 29 Data Protection Working Party [3]. Some main *principles in biometric usage proclaimed* in the opinion are noted below.

First, a clear determination of the *purpose* for which the biometric data are collected and processed. Processing of biometric data may only be lawful if all the procedures involved–starting from enrolment- are carried out regarding the law.

The principle of limiting the use of biometrics must be respected, among other *principles of personal data protection*; when defining the different purposes of an application, the principles of proportionality, necessity and data minimization must be respected in particular. Where possible, the data subject should be able to make choices between multiple purposes of an application with multiple functions, especially when one or more of them require biometric data processing.

Using biometrics additionally raises the question of *proportionality* of each category of processed data in the purpose's light for which the data are processed. Biometric data may only be used if adequate, relevant and not excessive. This implies a strict assessment of the necessity and proportionality of the processed data. The problem is also connected with the fact that biometric data often contain more information than that which is necessary for identification or authentication/verification functions.

Finally, it should be mentioned that the use of biometric systems might be constructed in such a way that they could be *privacy enhancing technology*.

Attention to the General Data Protection Regulation (GDPR) has to be paid as a concrete application of the above principles.

One of the most revolutionary aspects of the GDPR is the fact that it regulates biometric data as a separate entity rather than trying to include it in an existing privacy scheme that does not take into account biometric data sensitivity. Specifically, biometric data is defined as “personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allows or confirms the unique identification of that natural personal, such as facial images or dactyloscopy data” [4].

3. The court and biometrics

3.1. The California court decisions on governments possibilities to compel the use of body parts to unlock phones and other devises

The Government has applied for a search and seizure warrant to seize various items presumed to be at a residence in Oakland, California connected to the two suspects. The Application further requests the authority to seize various items, including electronic devices, such as mobile telephones and computers. The Government, however, also has to seek the authority to compel any individual present at the time of the search to press a finger (including a thumb) or use other biometric features, such as facial or iris recognition, for unlocking the digital devices found to permit a search of the contents as allowed by the search warrant.

If, however, law enforcement violates another constitutional right while executing a warrant, it inherently renders the search and seizure unreasonable. Even if probable cause exists to seize devices located during a lawful search based on a reasonable belief that they belong to a suspect, probable cause does not permit the Government to compel a suspect to waive rights otherwise afforded by the Constitution, including the Fifth Amendment right against self-incrimination. The Fifth Amendment provides that no person "*shall be compelled in any criminal case to be a witness against himself*." Citizens do not contemplate waiving their civil rights when using new technology, and the Supreme Court has concluded that, to find otherwise, would leave individuals "at the mercy of advancing technology."

The Court has found that using a biometric feature to unlock an electronic device is not akin to submitting to fingerprinting or a DNA swab, because it differs in two fundamental ways. First, the Government concedes that a finger, thumb, or other biometric feature may unlock a device in lieu of a passcode. In this context, biometric features serve the same purpose of a passcode which is to secure the owner's content, pragmatically rendering them functionally equivalent. Second, requiring someone to affix their finger or thumb to a digital device is fundamentally different from requiring a suspect to submit to fingerprinting. [5]

3.2. The Illinois case

The Illinois Supreme Court was ultimately unconvinced by the argument, ruling that a *person need not have sustained actual damage beyond the violation of his or her rights under the Act*. The court recognized that, through BIPA, the legislature had codified an individual’s “right to privacy in and control over their biometric identifiers and biometric information.” Whatever expenses a business might incur to meet the law’s requirements, the ruling reads, are likely to be insignificant compared to the substantial and irreversible harm that could result if biometric identifiers and information are not properly safeguarded. (Rosenbach v. Six Flags). Which serious progress from 2016 in US case law when the United States Supreme Court has held that for an aggrieved party to get damages through a violation of the statute, they *must allege an actual injury or adverse effect, and not just a technical violation* of the statute (Spokeo Inv v. Robins, 136 S. Ct 1540, 2016).

3.3. The EU cases

The creation of national dactyloscopy databases of all identity and residence cards holders would constitute a grave interference with the right to respect for private and family

life (Article 7 of the Charter) and with the right to protection of personal data (Article 8 of the Charter). There is no analysis which would demonstrate the necessity and proportionality of such grave interference. Whereas the proposal does not provide a legal basis for setting up or maintaining national databases, it could be clearer in ensuring that Member States do not use the biometric data collected for the purposes of the regulation to feed national biometric databases – at least as long as the proportionality and necessity of such processing is demonstrated in light of the strict requirements established by the EU data protection acquits [6].

Europe's migration and security challenges have prompted the European Union (EU) to develop and enhance multiple large-scale information technology systems (IT systems). Such systems provide invaluable support to border management efforts, but also cause wide-ranging fundamental rights issues [7].

The Highest Court in the European Union has paid more attention so far on investigating the legality of a European Union regulation requiring biometric passports in Europe and the electronic passports and biometric incorporated in them.

The Court of Justice of the EU (CJEU) has taken a great deal on way of gathering and proceeding biometrics (mostly fingerprints) under the Eurodac Regulation No 603/2013. The CJEU has confirmed in its case law that the fundamental right to dignity is part of EU law. People may perceive the *taking of their biometric features in an unpleasant way*, as noted by an expert interviewed by FRA. Refusals to provide fingerprints happen mainly in the context of Eurodac and less in relation to borders, visas or return processes. Article 1 of the EU Charter of the Human Rights of the European Union states that human dignity is inviolable and that it must be respected and protected. Article 1 is the foundation of all fundamental rights in the Charter.

4. Conclusions

The biometrics and biometric data always will be a delicate issue. Undoubtedly, their security is important. However, other issues remain in the background. This large set of questions concerns the capture and use of biometric data by governments.

Biometric systems provide a valuable service in helping to identify individuals from their stored personal details. Unfortunately, with the rapidly increasing use of such systems, there is a growing concern about the possible misuse of that information. To counteract the threat, the European Union (EU) has introduced comprehensive legislation that seeks to regulate data collection and help strengthen an individual's right to privacy [8].

In the EU context Opinion 3/2012, GDPR and Eurodac have made some movement towards standardizing the protection of biometric data when it created heightened requirements for collecting sensitive data. But all of them remain out of the center of the problem, because EU regulations are centered on biometric applications for verification.

The search for answers to important issues relating to the opposition to fundamental human rights and constitutional rights and law enforcement in biometric data is noticeable in the US legislation and the case law

This is an Open Access article distributed under the terms of the Creative Commons Attribution License

1. Roberg – Perez, S. Biometric Information and Data Privacy, Antitrust, Vol. 31, No. 3, Summer 2017, ABA, pp 60-65
2. Illinois Biometric Information Privacy Act*,* "Public Act 0994 95TH GENERAL ASSEMBLY"*,* www.ilga.gov, Retrieved 2018-05-07.
3. Opinion 3/2012 on the development of biometric technologies of the Article 29 Data Protection Working Party, 00720/12/BG WP193, publication available from http://ec.europa.eu/justice/data-protection/index_en.htm
4. Monajemi, M. Privacy Regulation in the Age of Biometrics That Deal With a New World Order of Information, University of Miami International and Comparative Law Review, 2018 pp 372-406, publication available from https://repository.law.miami.edu/cgi/viewcontent.cgi?article=1313&context=umiclr
5. Conclusion under Case No 4-19-70053 issued January 10, 2019, U.S. DISTRICT COURT, NORTH DISTRICT OF CALIFORNIA, OAKLAND OFFICE, available from https://assets.documentcloud.org/documents/5684083/Judge-Says-Facial-Recognition-Unlocks-Not.pdf
6. Fundamental rights implications of storing biometric data in identity documents and residence cards Opinion of the European Union Agency for Fundamental Rights (FRA Opinion 3/2018), Sept. 2018, publication available from https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-opinion-biometric-data-id-cards-03-2018_en.pdf
7. Under watchful eyes: biometrics, EU IT systems and fundamental rights, Luxembourg: Publications Office of the European Union, 2018 publication available from https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf
8. Bustard, J. The Impact of EU Privacy Legislation on Biometric System Deployment: Protecting citizens but constraining applications. IEEE Signal Processing Magazine, 32(5), 101-108, 2015, publication available from https://doi.org/10.1109/MSP.2015.2426682.