DOI 10.26521/Profuturo/2019/3/5769

Ferenc Zoltán Simó*

Then and now: laws on first and second generation biometric systems

Abstract

Although the security benefits biometric systems offer to our society, their widespread application can involve and clearly lead to serious legal issues and concerns, including technological encounters, disputes and grave concerns for individual citizens' rights of privacy. Various forms of identification, such as driving licenses, passports, and other identity cards, are progressively being combined with biometric information used by ever-changing and more advanced systems. With no doubt, it can be stated as well that the use of them will be spread to other sectors too. Therefore, it is safe to assume that this noticeable prosperity of personal information will involve and ache for more advanced data protection measures, encryption technologies, and other safeguarding measures, both to inspire their acceptance and use by the civilian population and to keep this critical information from falling into the wrong hands.

Keywords: *biometric systems, privacy legal concerns, biometric data*

Absztrakt

Habár a társadalom számára a biometrikus rendszerek kétségkívül nagy jelentőségűek és biztonságtechnikai szempontból tagadhatatlan előnyöket nyújtanak, nem szabad elfelejtenünk, hogy e rendszerek használatakor a magánszférát egyre fokozottabban érintő kockázatok jelenléte is kétségbevonhatatlan. Ezen kockázatok figyelembevétele és maguknak a rendszereknek az alapos és részletes ismerete szükségesnek tűnik ahhoz, hogy a felmerülő problémák jogi megoldásai is követhessék a szinte feltartóztathatatlanul terjedő és fejlődő technológiákat. Minél több szektor szánja rá magát a biometrikus rendszerek használatára, annál markánsabban jelentkezhetnek a magánszférát érintő kockázatok is, például adatvédelmi, illetve kódolási problémákat illetően.

Kulcsszavak: *biometrikus rendszerek, magánszféra-védelem, adatvédelem*

Most legal scholars, for example, *Tamás Klein, András Tóth, Attila Péterfalvi* and *Balázs Révész,* who are well-versed in technology and its latest achievements discuss and examine biometrics, biometric systems, phones, and drones separately as if they were not aware of the fact that most devices mentioned can communicate with each other or can even cooperate to achieve and execute complex tasks. Also, it may appear that scholars keep forgetting that scientists work day and night to invent and develop novel technologies. Although their work is comprehensive and sophisticated, *Tamás Klein* and *András Tóth*[1] do not discuss (in depth) the so-called second generation biometrics. It may sound as a work of science fiction, but, in fact,

* Ferenc Zoltán Simó, PhD student, Géza Marton Doctoral School of Legal Studies University of Debrecen (Hungary) Faculty of Law, simofredz@gmail.com.

[1] Klein, Tamás–Tóth, András (eds.): Technológiai jog – Robotjog – Cyberjog. Wolters Kluwer, Budapest, 2018. The authors focus on two aspects of novel innovations: "disruptive" and "unknown" innovations, but they

it is reality. One of the best examples may be telephones, as we have been calling them for decades, but phones, to be frank, are no longer *"simple"* caller and receiver devices, but sophisticated computers, cameras, data bases, and calculators (to name some) as well. They can also be connected by other phones and other devices using biometrics. Thus, even if I discuss them in separate chapters, I incline to bear in mind that they should be dealt with caution, since those technological devices can be interconnected or even controlled by an artificial intelligence (AI), which now is a bare fact and not a chapter in a piece of literature any more. Ultimately, I intend to focus on the examination of normative regulation with an emphasis on the legal reaction evoked by (novel) technologies.

1. An introduction: application(s) of biometric technology and preliminary observations on biometrics

Biometric characteristics have been used for a long time to identify or categorize known or unknown individuals. Biometric systems are different from the former use of unique or distinctive human features in that nowadays systems are capable of accumulating the unique and persistent/distinctive characteristics for computerized comparisons. Biometric systems are relatively novel, their rapid development started only some decades ago. But these highly complex systems and their functioning are mostly understood by only experts. Meanwhile, it cannot be denied that biometric systems have been set up and pioneered in extremely large-scale implementations, meeting a societal requirement for more security and able / professional cooperation.

Predominantly, it is well-known that these systems have been installed by the governments primarily focused on third country nationals, for example, on foreigners, such as asylum seekers or applicants for visas. Launching systems, such as Eurodac and VIS, were intended to investigate and observe criminals by SIS and SIS II. Also, biometric systems have steadily been expanding to the European Union and Member State nationals, for instance, the introduction in 2004 of the biometric ePassport in the EU Member States without reflective public responds or disputes then. Additionally, the rationale of these systems has been formulated or, if the original purposes were limited, the purposes and access to the databases were in several cases expanded, as in the case of VIS.

In addition, biometric systems have already been and are still coming in everyone's day to day life in the private sector, every now and then at a young age, for example, for access control in schools, which may raise even more privacy concerns than ever before, although the purpose or intention of the formerly mentioned example seems clear. To facilitate the debate about the use of biometric systems, including an analysis of its legal aspects, a "plain" understanding of the functioning of biometric systems (at least, for the legal and public sector) and of their main features, including of some more technical aspects as well, is supposed to be

mostly center their attention on legal challenges in connection with technological innovations and related issues such as data protection, robots, cyber law and drones.

mandatory but, as it can be seen, is often absent. But, it seems that biometrics have captured the attention of the private and legal sector, and the debate regarding privacy concerns has already started to heat up all around the world. Or, as *Els J. Kindt* notes, the results might be offered by a biometric system are for each use and application different and, it should be admitted that they are not "plug and play" and, since these systems are primarily based on measurements and statistical methods, with (obvious) standard errors (being inherent), these considerations must be taken into account as well.[2] Also, with bearing in mind that because of the intra-class and interclass variability of the characteristics measured, the comparison can never be 100%,[3] even if the technology has been developing rapidly with no slowing down in the horizon, thus one may state that biometric systems stay "inherently fallible." This fact may lead us to our privacy concerns as well, since one needs to understand that biometric systems error rates are not apt to offer 100% security or convenience and that the efficiency for this reason is sometimes questionable. And, of course, the accuracy which can be attained with biometric systems therefore remains (highly) conditional or uncertain.

2. Privacy and (any) technology

There might be an endless list of major concerns representing the troublesome relation between novel technologies and privacy. There is no doubt, and it seems obvious that it derives from two facts that were acknowledged long ago. First, the unstoppable nature of (high) tech development and the subjective nature of the concept of privacy, and second, as the clash of titans, these two are at a constant adjustment and readjustment to "live together" in peace, or rather in a status quo.[4]

Jane E. Kirtley argues that *"[p]rivacy is a subjective, and therefore, elusive, concept. Invoking it can create unlimited opportunities for mischief and genuine damage to public welfare. Ignoring it can undercut the individual's right to determine what his or her identity and destiny will be."*[5] Considering the illusiveness of the concept of privacy and the ever-changing, fast-pacing nature of technology together may offer us some insights in order to come up with a "relationship" or a "cooperation" that might actually work without creating more and more concerns. Probably it is not far-fetching to claim that technology, let alone "novel" technology, and its concept is as elusive as the concept of privacy.[6] And, of course, there may not be any hope for

[2] Kindt, Els J.: *Privacy and Data Protection Issues of Biometric Applications – A Comparative Legal Analysis.* Springer, Dordrecht, 2013. (doi: 10.1007/978-94-007-7522-0).

[3] Though I do not aim to state that there is the slightest chance to guarantee a system with 100% infallibility.

[4] See, for example, Wright, David–De Hert, Paul (eds.): *Enforcing privacy – Regulatory, Legal and Technological Approaches.* Springer, New York, 2016. (doi: 10.1007/978-3-319-25047-2).

[5] Kirtley, Jane E.: Introduction. In: Anglim, Christopher (ed.): Privacy Rights in the Digital Age. Grey House, Amenia, 2016, XXVI.

[6] See Jiang, Richard–Al-maadeed, Somaya–Bouridane, Ahmed–Crookes, Danny–Beghdadi, Azeddine (eds.): *Biometric Security and Privacy – Opportunities & Challenges in The Big Data Era.* Springer, New York, 2017. (doi: 10.1007/978-3-319-47301-7).

anyone to come up with a unified definition of both. As far as biometric systems are concerned, it seems that the (re)definition of the notion of them is an ongoing project.

3. Short history of biometrics

Nowadays technology is universally recognized as an integral component of social change. Moreover, it is increasingly approved and agreed that technology cannot be understood outside its social context. Historians, and especially historians of technology, have come to distinguish the role that cultural, political, and economic values have played in shaping technological improvement / novelty, as well as the role that technological innovation has played in determining values. Such a "contextual" appreciation of technology is part of a larger endeavour to understand and control the interactions of technology and law as well. Hence, a better understanding of our technological past may be able to contribute to the practical end of revealing / uncovering technology.

The twentieth century witnessed a historic change in the relationship between science and society. In the so-called trench war, World War I, scientists were recruited and died in the trenches. In World War II they were excused as national treasures and committed to the utmost secrecy, and they united behind their country's war effort, and, of course, they devoted their lives to the "cause." The explanation of the change is not difficult to find, since governments were ready to consider and realize that theoretical research could produce practical progress in industry, agriculture, medicine and almost all walks of life, but having been in a hurry, they hardly pondered upon, and never imagined that one day, in the post-war future, the Pandora's box they had opened would not be able to be shut. It was not realized that without progressive legal attempts to regulate novel technologies, it would become the source of serious (legal) concerns. Their belief was firmly strengthened by improvements such as the discovery of antibiotics and the application of nuclear physics to the production of atomic arsenals. Science became identified with practical profit and benefits and the dependence of technology on science is universally supposed to be an eternal affiliation and a solitary enterprise.[7]

Thus, science and technology, research and development, all four are seen to be as inseparable as twins. The conviction in the pairing of science and technology is now petrified in the dictionary definition of technology as applied science. When we talk about technology, we usually think about novelty and the future. For many decades now the term "technology" has been closely linked with invention (the creation of a new idea) and innovation (the first use of a new idea). Talk about technology centres on research and development, patents and the early stages of use, for which the term diffusion is used. The timelines of technological history are based on dates

[7] See Stuart, Casey-Maslen: Pandora's box? Drone strikes under jus ad bellum, jus in bello, and international human rights law. *International Review of the Red Cross,* 2012, 597–625. (doi: 10.1017/S1816383113000118); McGuire, James E.–Tuchanska, Barbara: *Science Unfettered – A Philosophical Study in Sociohistorical Ontology.* Ohio University Press, Athens, 2000.

of invention and innovation.[8] The most important 20th century technologies are often abridged to the following examples: flight (1903), nuclear power (1945), contraception (1955), and the well-known Internet (1965).[9]

It is frequently said that change is taking place at an ever increased speed, and that the new is increasingly influential, and, in addition, technology is always faster than the reaction to its influence on the society.[10] Also, it is supposed that societies are really slow to adapt to novel technologies, and the list of novelties is expanding, by now it consists of many, such as biometrics, drones, smart phones, and so on. However, before the reign of technology and its progress, it was admitted that some parts of our body could be used to identify our unique selves, thus the ideas does not seem novel at all. Since prints of hand, foot and finger have been used in ancient times due to their unique characteristics. Since it is not my primary aim to create a timeline, I mention only a handful of them with no intention to give a full account.

The Babylonian King *Hammurabi* (1792–1750 BC) is known to have enacted one of the first written codes of law in the world in clay tablets. The kings of Babylon were allegedly using an imprint of their right hands in the clay tables in order to authenticate the tables.[11] Among other things, in Babylonia, fingerprints were also used in business transactions that were recorded on clay tablets. It is also a well-known fact that the Chinese have used fingerprints and handprints as marks of authenticity for at least 2,000 years. In ancient China, fingerprints were customarily pressed in clay tablets and clay seals. Documents from the Tang dynasty in China (618–907) referred to the use of fingerprints and handprints on contracts.[12] These examples can be seen as the earliest attempts to identify or verify the identity of an individual, and I include them in order to draw attention to the fact that though the idea of improving identification started long ago, it seems that we did not have the time to prepare for the revolution of technology, which might have begun for the most part in the 19th and the early 20th century.

4. Introduction to biometric systems

Although a layperson might have some information on what biometrics or biometric systems may mean, no-one is expected to be an expert on these systems, even if people use them more and more often with having prior knowledge on them. Thus,

[8] See Kendall, Diana: *Sociology in our times.* Wadsworth, Belmont, 2003; Klein–Tóth: *op. cit.*

[9] See Cumo, Christopher: *Science and technology in 20th-century American life.* Greenwood Press, London, 2007; Channell, David F.: *A History of Technoscience Erasing the Boundaries between Science and Technology.* Routledge, London, 2017. (doi: 10.4324/9781315268897).

[10] Headrick, Daniel R.: Technology – A World History. Oxford University Press, New York, 2009.

[11] See Ashbourn, Julian: The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies. *Background paper for the Institute of Prospective Technological Studies,* DG JRC – Sevilla, European Commission, 2005. http://www.statewatch.org/news/2005/apr/jrc-biometrics-julian-ashbourn.pdf; 4. (09. 01. 2019).

[12] Farelo, Antonio: A History of Fingerprints. Interpol, April 2009. http://www.interpol.int/Public/Forensic/fingerprints/History/BriefHistoricOutline.pdf; 2. (09. 01. 2019).

for the purpose of my study, I endeavour to highlight some basics of biometrics or biometric systems.

A biometric system measures one or more physical or behavioural characteristics, including fingerprint, palm print, face, iris, retina, ear, voice, signature, gait, hand vein, odour, or the DNA information of an individual to determine or verify one's identity. These characteristics are referred to by different terms such as *traits, indicators, identifiers,* or *modalities.*

The ability to identify individuals uniquely and to relate personal attributes, for instance name, nationality, to an individual, has always been essential to the fabric of human society. Humans normally use body characteristics (such as face or voice) and bear other contextual information (such as position or outfits) to recognize one another. The set of attributes associated with a person constitutes their personal identity. In the early days of civilization, people lived in small communities where individuals could easily recognize each other, and a stranger among them was easily recognizable. However, an explosion in population growth accompanied by improved and more flexible mobility in modern society has demanded the development of sophisticated identity management systems that could efficiently record, maintain, and eliminate personal identities of individuals.

Identity management plays a significant role in several applications. Examples of such applications may include regulating international border crossings, limiting physical access to key civilian and military facilities, such as nuclear plants or airports, controlling logical access to collective resources and information, performing remote financial transactions, or distributing social welfare benefits. The spread of web-based services, for instance, online banking and transactions, and the deployment of decentralized customer service centres, for instance, credit cards have shown the way to the risk of identity theft.[13]

I also add that it seems important that the term biometrics is often criticized by experts on this field, for example, *Anil K. Jain, Arun A. Ross* and *Karthik Nandakumar* argue that the term *biometric recognition* is possibly more appropriate than biometrics because the latter has been historically used in the field of statistics to refer to the analysis of biological (particularly medical) data.[14] In order to clarify the importance of biometrics, first we need to turn to the origin of the term. The term *biometrics* derives from the ancient Greek *bios* = "life" and *metron* = "measure." Biometrics refer to the entire class of technologies and techniques to uniquely identify humans. Although biometric technology has diverse applications, the most crucial purpose of it is to provide a more secure alternative to the traditional access-control systems used to protect personal or corporate assets. Biometric systems apply facial images, fingerprints, iris and/or voice in a computerized way to identify or to confirm (identity) claims of persons. It is completed on the basis of the automated measurement and analysis of their biological characteristics (such as fingerprints, face, iris

[13] Identity theft or identity fraud occurs when a person usurps the identity of another individual or claims a false identity in order to access resources or services to which he is not entitled.

[14] Jain, Anil K.–Ross, Arun A.–Nandakumar, Karthik: Introduction to Biometrics. Springer, New York, 2011, 1–3. (doi: 10.1007/978-0-387-77326-1).

or even ear[15]) or behavioural characteristics (such as signature or voice). Biometric technology has been used for some time in civil applications on a small scale for access control purposes to places which require an enhanced / advanced security, such as to military and nuclear facilities or bank vaults, but is now gaining increased interest from governments and the private sector as well.

While a heated debate has already emerged about whether conventional biometric technology can offer society any significant advantages over other forms of identification, and whether it represents a (considerable amount of) threat to privacy, technology is progressing fast. Moreover, it is striking to see how politicians and the public are still discussing fingerprinting and iris scan, while scientists and engineers have already started testing futuristic (though realistic) solutions. These are the so-called *second generation biometrics,* which include multimodal biometrics, behavioural biometrics, dynamic face recognition, EEG and ECG biometrics, remote iris recognition, and other, still more astounding, applications, is a reality which promises to turn over any current ethical standard about human identification. Robots which are capable of identifying their makers/masters, CCTV which is able to "sense" intentions, voice responders which have the ability to evaluate/analyse emotions: to be frank, these are only some applications in progress to be developed further.

Knowing all this, it might be evident that legal certainty has arisen, but, there is no consensus but legal uncertainty on many aspects of its use.[16] Currently, biometric technologies play a primary role in security, immigration and border control policies of the European Union, in particular in large-scale systems, such as Eurodac or VIS. Before looking at the different known methods, a review of why at all bother using the ear as a biometric will be examined. In order to make a biometric characteristic practical, the following seven properties must be valid to some degree:[17]

(1) Universality: it means that every person should have the biometric characteristic;
(2) Uniqueness: no two persons ought to be the same in terms of the biometric characteristic;
(3) Permanence: the biometric characteristic should be invariant over time;
(4) Collectability: it implies that the biometric characteristic should be measurable with some (practical) sensing device;
(5) Performance: the technology applied should have a certain accuracy, speed, and robustness (often associated with validity);
(6) Acceptability: the particular user population and the public in general should have no (serious) objections to the measuring / collection of the biometric;
(7) Circumvention: which entails that the technology should be ease of use of a substitute.

[15] Using the ear as a biometric modality is a newcomer in the fields of biometric recognition techniques. There are relatively not many ongoing researches within this topic, in which most of them deal with investigating unused methods in order to improve the performance. Therefore there is yet no well-established fully automated ear recognition system.

[16] See Strandburg, Katherine–Stan Raicu, Daniela (eds.): *Privacy and Technologies of Identity – A Cross-Disciplinary Conversation.* Springer, New York, 2006. (doi: 10.1007/0-387-28222-X).

[17] Jain, Anil K.–Ross, Arun A.–Prabhakar, S.: An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology,* 2004/1, 4–20. (doi: 10.1109/TCSVT.2003.818349).

With the increasing concerns on security breaches and transaction fraud, highly reliable and convenient personal verification and identification technologies are more and more requisite in our social activities and national services. Biometrics, used to recognize the identity of an individual, are gaining ever-growing popularity in an extensive range of governmental, military, forensic, and commercial security applications.[18]

In addition, biometrics is used mostly for authentication and identification by governments, employers, and various service providers. Data collection is easily done and does not require cooperation or awareness of the target. Government agencies, particularly law enforcement agencies, are the largest data collectors. It is also well-known that the U.S. government operates and preserves some of the largest biometric identification systems in the world. The Department of Homeland Security (DHS) maintains an automated biometric identification system (IDENT). IDENT sustains a database of more than 126 million records and conducts about 250,000 biometric transactions, averaging 10 seconds or less per transaction, each and every day.[19] The DHS Biometric Optical Surveillance System (BOSS) performs real-time facial recognition and has the capability of capturing iris data from a target 10 meters away even while the individual is on the move.[20]

Since biometric technology has expanded, the capacity to store and disseminate the collected data has increased significantly. Most local and national law enforcement agencies seek to make the communication between their various databases flawless and responses to inquiries fast and precise. The ability to integrate and store information from numerous different databases has dramatically increased the value of biometric data to organizations. However, it has also radically increased the risks that come with collecting and maintaining it. Privacy advocates expressed their great concern about the use of biometrics in law enforcement. With the combined use of surveillance tools such as facial recognition technology, many fear that the United States is entering a regime of pervasive, large-scale surveillance.

The application of biometrics does entail various and serious privacy risks, including identity theft, function creep, and government surveillance. There is greater safety and convenience in using biometrics rather than older forms of personal recognition. In some cases, biometrics may be used to replace or supplement the existing technology. In other cases, biometrics is the only viable approach given the circumstances. Biometrics is better than traditional recognition in several different cases. In some applications, it either replaces or supplements existing technologies; in others, biometrics is the only sensible approach to personal recognition. As the infrastructure for dependable automatic personal recognition goes on to be developed along with the ability to associate an identity with other personal behaviour, privacy advocates articulate increasing concern that this information might violate individual privacy rights.

[18] See Strandburg–Stan Raicu: *op. cit.*

[19] Taylor, Mark: *Genetic data and the law – A critical perspective on privacy protection.* Cambridge University Press, Cambridge, 2012. (doi: 10.1017/CBO9780511910128); Campisi, Patrizio (ed.): *Security and Privacy in Biometrics.* Springer, New York, 2013. (doi: 10.1007/978-1-4471-5230-9).

[20] Puniskis, Michael J.: Biometric Center of Excellence (BCOE). In: Anglim: op. cit., 42–43.

A human physiological or behavioural trait might be a biometric characteristic if it meets the following criteria: first, the trait must be universal, which simply means that each person has the characteristic; second, it must be distinctive, thus the characteristic is unique for each person; third, the trait must be permanent, which basically means that the characteristic ought to be adequately invariant, that is, it must match the criterion over a certain period of time; and fourth, it needs to be collectible, meaning that the characteristic ought to be quantitatively measurable. Practically, it means that a functioning biometric system must reach acceptable levels of performance, acceptability, and circumvention. But, it seems crucial as well that it must also be sufficiently strong and be capable of resisting a great variety of fraudulent methods and attacks.

A biometric system uses pattern recognition to recognize a particular person based on a specific physical or behavioural characteristic possessed by a particular person. Depending on the application context, a biometric system typically operates in one of two modes: verification mode or identification mode. In the verification mode, the system confirms the person's identity by comparing the captured biometric characteristic with the individual's biometric template, which is stored in the system database. According to *Christopher Puniskis*, biometrics raises several concerns. The first one is unintended functional scope. He assumes that it can easily happen because biometric identifiers are biological in origin; it seems very likely that collectors may pick up additional personal information from the biometric measurements. The second might be unintended application scope. The assumption is that strong biometric identifiers such as fingerprints allow for probably unwanted and unnecessary identifications. The last one is covert recognition. A biometric sample, such as a person's face, may and could be retrieved without the target person knowing or realizing it.[21] Of course, this leads to the conclusion that individuals who intend to keep their anonymity could have their privacy rights violated by biometric recognition.[22] He also argues that prevention is also achievable, thus, abuse of biometric information (or its derivatives) can be prevented or mitigated through the application of a number of methods: *"1. Government legislation and regulation. The European Union (EU) has already adopted legislation against sharing biometric identifiers and personal information. 2. Assurance of self-regulation. A group of biometric vendors could join to agree to be bound by ethical guidelines in their operations. 3. Autonomous enforcement by independent regulatory organizations, such as a central biometrics agency."*[23] Of course, several institutions have been established in order to assume better understanding and promote novel tech such as biometrics. Thus, the introduction of some is of primary importance for our purpose.

[21] For example, a drone can be easily used to achieve "relative invisibility" to get close enough to a target person without being revealed or discovered.

[22] Anglim: op. cit., 46–47.

[23] Ibid.

5. Biometric Center for Excellence (BCOE) and Biometric Optical Surveillance System (BOSS)

The Biometric Center for Excellence was established in the USA in 2007 by the Science and Technology Branch of the Federal Bureau of Investigation (FBI) in order to survey, advance and expand the use of new and enhanced biometric technologies, capabilities, standards and policies, for integration into operations. Its overall mission is to reinforce criminal investigative potential and augment national security. Coming from a need to advance and manage the growing biometric activities and priorities of the FBI more efficiently, the BCOE[24] is fundamentally a consortium of the services and expertise of three divisions, the Criminal Justice Information Division, the Laboratory Division and the Operational Technology Division, intended to promote collaboration, improve and support information sharing and advance the adoption of optimal biometric and identity resolutions. This collaboration assists to abolish a major challenge the capability gap by providing available biometric capabilities while assessing future needs. Outside the FBI, on a regular basis the centre works with the Office of the Director of National Intelligence, the Department of Homeland Security, the Department of Defense and the Department of Justice, as well as other law enforcement agencies and national security communities. The BCOE also sponsors research, evaluates technologies, develops training, establishes standards, and certifies biometric products. The BCOE addresses privacy and procedural and policy issues related to the use of biometric systems while working in compliance with privacy laws, policies, and regulations.

One of the systems aches for mentioning is BOSS, Biometric Optical Surveillance System.[25] It is a system with the capacity to recognize faces and match them with personal identification information. Government agencies and federal, state and local law enforcement developed BOSS to store and utilize this data legally, as needed. Government agencies, particularly public safety agencies, are major collectors of data. The U.S. government operates some of the largest biometric identification systems in the world. As mentioned above, DHS maintains an automated biometric identification system (IDENT) that have a database of more than 126 million records and conducts 250,000 biometric transactions per day.

Even though, especially American citizens have a great expectation of privacy, this right, as in the European Union, is legally balanced against the needs for public safety and national security. Personal information is stored, linked and shared among law enforcement agencies to guarantee and assure public safety, but this use might involve some trade-offs in terms of individual privacy. *Cyber-tampering* is an existing risk based on how much and how often this information is used and protected. Inadequate security could allow criminals to access this information (even from great distances) and allow personal identification information to be seriously compromised.

[24] Puniskis: op. cit., 42–43.
[25] Anglim: op. cit., 44–45.

In additions to these considerations, the aggregation and accumulation of data from several different sources can pose a serious privacy threat. The theft of biometric information could aid criminal access to bank accounts and credit cards, and, for instance, there can be a danger of data creep, where information willingly provided to one law enforcement agency may possibly be transferred without permission to another government agency, then linked with other data or applied to a new and unauthorized purpose (even with or without being recognized). At the same time, the unfettered scope of data collection, sharing, linking and storing could invite misuse. Law enforcement officials are aware of the risks involved in the usage of BOSS. They trust that the government surveillance is necessary in these instances and requires support.

As I have formerly mentioned, there are several concerns to be addressed and many of them have already surfaced by the revolution of novel technologies. *Shaunté Chácon* poses and attempts to answer a serious question when he asks: *"How should BOSS be regulated so that the legitimate privacy rights of U.S. citizens are not violated?"*[26] He states that one of the proposals is to limit access to BOSS as much as possible. Two policies are essential to provide adequate parameters for BOSS. First, facial recognition databases ought to use exclusively images of known terrorists and convicted felons. Driving license photos and other images of innocent people should never be included in a facial recognition database without the knowledge and consent of the public. Second, access to databases should be limited and monitored.[27]

As far as Europe and the European Union are concerned, we can see that the situation may seem a bit grievous. The European Union has a significant legal data protection framework, built up around Directive 95/46/EC,[28] the General Data Protection Regulation (GDPR),[29] Directive 2016/680[30] and the Charter of Fundamental Rights. Still, the question of whether data protection and its legal framework are "in good health" is increasingly being posed. Advanced technologies raise fundamental issues regarding key concepts of data protection. Falling storage prices, increasing chips performance, the fact that technology is becoming increasingly embedded and ubiquitous, the convergence of technologies and other technological developments are broadening the scope and possibilities of applications rapidly. Society however, is also changing, affecting the privacy and data protection landscape. The "demand" for free services, security, convenience, governance, for example, changes (even if

[26] Chácon, Shaunté: (BOSS). In: Anglim: op. cit., 45.

[27] Chácon: op. cit., 43–45.

[28] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31–50) in force until 25 May 2018.

[29] 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) (OJ L 119, 4.5.2016, p. 1–88).

[30] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89–131).

they seem slight or trivial) the mind-sets of all the stakeholders involved. Privacy is being proclaimed dead or at least worthy of dying by the captains of industry; governments and policy makers have to manoeuvre between competing and incompatible aims; and citizens and customers are considered to be indifferent.

6. Multi-biometrics[31] – A brief introduction

As I have already discussed, it can be reaffirmed that systems of personal recognition are usually based on individual biometric traits, such as, face, iris and fingerprint, have been the focal point of my research so far. Most of these biometric systems could be categorized or characterized as uni-biometric systems for the reason that they rely on a single biometric source for recognition. Any piece of evidence that can be independently used to recognize a person is called a *source* of biometric information. One of the topics that appears to be more and more often discussed is whether uni-biometric systems have or do not have some limitations. This needs to be considered for various reasons. One of the reasons is what if the biometric source becomes unreliable owing to some technical error, for instance, sensor or software failure, poor quality of specific biometric trait of the user, or intentional manipulation? Moreover, high-security applications and extensive civilian identification systems set rigorous accuracy requirements to be followed that cannot be met by existing uni-biometric systems. Multi-biometric systems on the other hand seem more than capable of handling the formerly mentioned obligations or conditions.

By definition multi-biometric systems of personal recognition are systems that combine and gather evidence from multiple sources of biometric information in order to determine, identify or verify the identity of an individual. For instance, face and iris traits, or fingerprints from all ten fingers of an individual might be used in concert to determine the identity of the person with reasonably high precision or accuracy. As it is often argued, multi-biometric systems are capable of triumph over several shortcomings of uni-biometric systems because the different biometric sources generally balance for the inbuilt or inherent limitations of one another. Therefore, multi-biometric systems are commonly supposed to be more reliable and accurate than uni-biometric systems, as well as to offer wider population coverage.[32]

The process of consolidating the information or evidence obtained by multiple biometric sources is known as *information fusion*. In order to improve precision, the so-called accuracy improvement, which is the prime impetus for applying multi-biometric systems, occurs as a result of at least two main reasons. Firstly, the fusion of multiple biometric sources effectively increases the dimensionality of the feature space and reduces the overlap between the feature distributions of different individuals. To put it differently, I assume that a combination or mixture of multiple biometric sources is seen more distinctive and capable of identification or verification to an individual than a single biometric sample. The second reason is that noise, inexactness, vagueness

[31] Jain–Ross–Nandakumar: op. cit.

[32] See also Jiang–Al-maadeed–Bouridane–Crookes–Beghdadi: *op. cit*.

or natural drift might be caused by factors like aging or an accident, in a subset of the biometric sources can be compensated by the discriminatory information given by the remaining sources. Thus, availability of multiple biometric sources provides redundancy and fault-tolerance in the sense that the recognition system continues to operate even when certain biometric acquisition modules fail.[33]

7. Conclusion

Despite the security benefits these technologies offer, their extensive application also involves and obviously leads to serious issues, including technological challenges, disputes and concerns for individual citizens' rights of privacy. Numerous forms of identification, such as driving licenses, passports and other identity cards are increasingly being combined with biometric information, and it can be stated as well that the use of them will be spread to other sectors too. Therefore, I assume that this visible prosperity of personal information will entail more advanced data protection measures, encryption technologies and other safeguarding measures, both to encourage their acceptance and use by the civilian population and to keep this critical information from falling into the wrong hands. Still, it cannot be overseen that biometric systems and data may be used by governments in many ways. Critics such as the American Civil Liberties Union are deeply concerned that such power might be easily abused for unethical or unlawful purposes. While biometric technologies have advanced rapidly, they are still given to technological deficiency or limitations, such as computer errors, "cog in the wheels" and glitches, which can misidentify individuals, leak sensitive or critical personal data and lead to other privacy-related issues.

[33] Jain–Ross–Nandakumar: op. cit., 211. It is also important to consider Campisi: op. cit. This work presents the latest secured and privacy-compliant techniques in computerized human recognition. Offering viewpoints from an international selection of experts in the field, the comprehensive coverage spans both theory and practical implementations, taking into consideration all ethical and legal issues. Its topics are unique with focusing on novel approaches and new architectures for unimodal and multimodal template protection; examines signal processing techniques in the encrypted domain, security and privacy leakage assessment, and aspects of standardization.