http://dx.doi.org/10.18623/rvd.v23.n4.4853

ELECTRONIC PASSPORTS: IMPORTANCE AND IMPLICATIONS

PASSAPORTES ELETRÔNICOS: IMPORTÂNCIA E IMPLICAÇÕES

Article received on: 10/9/2025
Article accepted on: 1/9/2026

Luz María García García*
*Technological Institute of Chilpancingo and Open and Distance University of Mexico, Mexico City, Mexico
Orcid: https://orcid.org/0000-0001-9443-9708
luz2g@yahoo.com.mx

Víctor Alberto Gómez Pérez**
**Systems and Computing, Technological Institute of San Juan del Río, San Juan del Río, Querétaro, Mexico
Orcid: https://orcid.org/0000-0002-7758-6690
victor.gp@sjuanrio.tecnm.mx

Saturnina Jiménez García***
***Universidad de la Sierra Sur, Miahuatlán de Porfirio Díaz, Oaxaca, Mexico
jimenezsaturnina10@gmail.com

Sonia Mendoza****
******Computer Science Department, Centro de Investigación y de Estudios Avanzados, Mexico City, Mexico
Orcid: https://orcid.org/0000-0002-4897-7756
sonia.mendoza@cinvestav.mx

Jesús Cruz Ahuactzi***
***Universidad de la Sierra Sur, Miahuatlán de Porfirio Díaz, Oaxaca, Mexico
Orcid: https://orcid.org/0009-0004-6351-2676
ahuactzi@unsis.edu.mx

Alejandro Jarillo Silva***
***Universidad de la Sierra Sur, Miahuatlán de Porfirio Díaz, Oaxaca, Mexico
Orcid: https://orcid.org/0000-0002-9776-6533
ajarillo@unsis.edu.mx

The authors declare that there is no conflict of interest

Abstract
The evolution of Information and Communication Technologies (ICTs) has enabled governments to deliver services to citizens more efficiently and effectively. This study conducts a literature review on electronic passports to examine the implications of biometric technology in their implementation. A qualitative methodology was adopted, based on documentary analysis of articles published in specialized academic journals. The findings indicate that biometric data used in electronic passports include facial recognition, fingerprints, and iris recognition. Additionally, continuous review and updating of technology are required to prevent potential forgery and identity theft.

Keywords: Biometric Data. Biometric Systems. Electronic Passport. ICT.

Resumo
A evolução das Tecnologias da Informação e Comunicação (TIC) tem permitido que os governos ofereçam serviços aos cidadãos de forma mais eficiente e eficaz. Nesse sentido, o principal objetivo deste estudo é realizar uma revisão da literatura sobre passaportes eletrônicos, a fim de examinar as implicações da tecnologia biométrica em sua implementação. Para alcançar esse objetivo, adotou-se uma metodologia qualitativa, baseada na análise documental de artigos publicados em periódicos acadêmicos especializados. Os resultados indicam que os dados biométricos utilizados nos passaportes eletrônicos incluem reconhecimento facial, impressões digitais e reconhecimento da íris. Além disso, é necessária a revisão e a atualização contínuas da tecnologia para prevenir possíveis falsificações e o roubo de identidade.

Palavras-chave: *Dados Biométricos. Passaporte Eletrônico. Sistemas Biométricos. TIC.*

1 INTRODUCTION

Electronic passports represent a significant advancement in governmental identity documentation. The integration of biometric technology into travel documents reflects the contemporary need for enhanced security measures at international borders. Governments worldwide have invested substantial resources to implement electronic passport systems, seeking to improve border control efficiency while maintaining traveler convenience.

The adoption of electronic passports stems from multiple governmental objectives: streamlining information sharing between agencies, facilitating international cooperation, and establishing transparent systems that serve citizens' needs effectively. These documents incorporate biometric data stored on embedded chips, raising important considerations regarding data protection and privacy. Governments bear the responsibility of implementing appropriate safeguards to ensure that citizens' biometric information remains secure and is used solely for authorized purposes.

This article examines the importance of electronic passports and their implications for governments. The following sections address the research methodology, biometric systems, electronic passports, biometric data, and conclusions.

2 METHODOLOGY

Electronic passports constitute a relatively recent concept lacking a dedicated theoretical framework. Instead, this field draws upon various interconnected concepts, including biometric systems and biometric data. This research employs a qualitative approach. The information collection process involved comprehensive searches through specialized academic journals and books to structure concepts and develop this theoretical investigation.

An exhaustive review was conducted across multiple bibliographic sources, including Scopus, Google Scholar, and official sources such as the International Civil Aviation Organization (ICAO). Additionally, key advances and strategies aimed at developing biometric system applications, particularly electronic passports, were explored.

3 BIOMETRIC SYSTEMS

Obardat et al. (2019) note that the history of biometric systems dates back to 1800. However, approximately 30 years ago, the field experienced slow evolution, with only a limited set of technologies, mostly physiological, being available. Danko and Fernández (2016) define biometric systems as automated methods of verifying or recognizing the identity of a living person based on physiological or behavioral characteristics.

Biometric systems operate in three distinct modes. First, enrollment creates a biometric template for users by capturing raw data and constructing a mathematical representation of corresponding biometric features. Second, verification validates a person's identity by comparing captured biometric data with templates stored in the system's database for the claimed identity; this forms the basis of authentication and access control systems. Third, the identification process recognizes actual individuals (OBARDAT et al., 2019).

These authors identify three types of biometric authentication approaches: static, active, and continuous authentication. Static authentication verifies an individual's identity once, typically at login. Active authentication re-authenticates the individual, generally occurring after initial login. Continuous authentication can occur periodically, following a certain amount of activity, or upon expiration of a predefined time interval.

Stenum (2017) identifies several factors driving the global increase in biometric technology markets: increased public spending, national identification projects, electronic passports and visas, cybercrime, rising crime rates, escalating terrorist activities, and data theft. This indicates that technological globalization requires society to adapt to new forms of surveillance and control. Through data stored on chips, individuals can be identified even when not physically present, as exemplified by electronic passports.

According to Obardat et al. (2019), biometric technology presents several types of failures. The False Acceptance Rate (FAR) represents errors resulting from confusing biometric measurements of two different people with the same identity. The False Rejection Rate (FRR) results from confusing two biometric measurements of the same person with two different individuals. The Failure to Capture Rate (FTCR) indicates the rate at which the system cannot process captured raw biometric data and extract features. Finally, the Failure to Enroll Rate (FTER) occurs when the system cannot enroll a user's biometric characteristics. These authors note that error costs vary by type; false rejection proves much less costly than false acceptance. Therefore, false rejection represents a source of frustration, while false acceptance constitutes a security breach.

Technological development has enabled the refinement and automation of biometric data processes, which allow for identifying or authenticating human identity through physiological or behavioral characteristics. Consequently, countries have incorporated this technology into electronic passports. The importance of biometric technology evolved rapidly, becoming a regulatory mechanism for different societal aspects, including security, economics, immigration control, and culture.

Muller (2011) points out that applying biometric technology in governments contributes to improving risk management in migration, mobility, and border control. Porwick (2009) notes that biometrics are integrated into driver's licenses, surveillance systems, health identity cards, and electronic passports. Currently, biometrics represents a fundamental security technique linking an individual's identity using methods that focus on diversity among members of a given population.

The evolution of ICT has enabled both populations and governments to advance by incorporating online services such as permit and license applications or electronic passports. Biometrics extends into the private sector in commercial systems, labor attendance tracking, and the banking sector to offer security services through data sharing. In the 20th century, biometrics was incorporated into immigration control through travel documents known as electronic passports (SANTI, 2017).

Entrust, formerly Datacard Group, is one company providing maximum security technology for electronic passports. This company supplies technologies to financial institutions, national governments, corporate enterprises, and other organizations to establish trusted identities and conduct highly secure transactions (ENTRUST, 2014).

This United States-based company provides technology to other governments as an easily deployable method for inspecting today's advanced machine-readable electronic travel documents (eMRTDs) at border security checkpoints.

4 ELECTRONIC PASSPORTS AND BIOMETRIC SYSTEMS

Díaz (2014) traces the evolution of passports, noting that the first ones appeared on Egyptian tablets due to relationships between Egypt and Asia. Officials were sent as messengers, usually of high rank, a practice that also applied to Greece. During the Roman Empire, those sent on missions carried documents certifying their identity and positions. However, no organized system of documents existed for traveler protection at that time. The first appearance of public policies regulating migratory flows began after feudalism's extinction at the end of the 15th century, following wars that arose in Europe.

Regarding the general concept of passports, ICAO (2010) defines them as documents issued by a State or organization on behalf of a State to its nationals or other persons for purposes of facilitating their travel abroad. Passports are intended to protect borders, privacy, and prevent identity theft. An electronic passport is defined as a Machine Readable Passport (MRP) with a contactless integrated circuit (IC) microprocessor that stores MRP data, biometric measurements of the passport holder, and security data (ICAO, 2010, p. 7).

According to Foucault (2014), the importance of using electronic passports for governments lies in control purposes, as governments possess the power to decide who can cross their borders. The International Civil Aviation Organization (ICAO, 2010) identifies advantages of implementing electronic passports: improving security and border control, combating terrorism and crime, and promoting secure travel worldwide. However, disadvantages exist for governments in countries that have already implemented them, such as the use of false identities to process travel documents, identity theft, the entry of terrorists across borders and at immigration offices, privacy issues, and the use of information for other purposes.

Electronic passports emerged as a strategy to prevent illegal immigration, terrorism, and organized crime. Furthermore, electronic travel passports allow for greater security measures because they cannot be easily forged or counterfeited; however, this

depends on the type of technology in which countries invest. Côté-Boucher (2008) mentions that electronic passport implementation responds to external threats related to international terrorism, transnational crime, and drug and human trafficking.

Gipp et al. (2007) note that electronic passports contain an RFID (Radio Frequency Identification) chip and Public Key Infrastructure (PKI) as aspects that reduce deception and protect international identification. An RFID system consists of two components: a transponder and a reader. In electronic passports, the transponder is the radio frequency chip (RFID chip) embedded in the document's body.

The number of migrants has increased considerably worldwide, but with ICAO's arrival as the main source of standards for international travelers, much of this phenomenon has been regularized. At this organization's first conference, proposals were introduced regarding machine-readable passports. These documents, in addition to containing paper, have a chip requiring no batteries, which protects user security. In 1968, ICAO established an advisory panel responsible for standardizing passports to make them machine-readable. A resulting standard was issued in 1978, focusing on optical character recognition to obtain essential traveler information through passport documents (DURAN, 2010).

Subsequently, the New Technologies Working Group (NTWG) examined biometric comparisons as a more authentic means in documents to compare printed or electronic data. In February 2002, the NTWG approved facial characteristics, fingerprint, and iris recognition technologies applicable to Machine Readable Travel Documents (MRTD). Later, in Berlin in June 2002, the NTWG approved facial recognition as a globally interoperable biometric for machine-assisted identity confirmation with machine-readable travel documents (WATKINS, 2007).

Electronic passports have become a primary tool for border control in countries, both for issuing and receiving nations. The Border Patrol Office (2004) defines operational border control as the reasonable certainty of apprehending terrorists, instruments of terrorism, illegal aliens, and smugglers between ports of entry or their means of illegal entry, and the detection and turnback or apprehension of those individuals from ports of entry considered high-risk.

5 BIOMETRIC DATA

According to Porwick (2009), biometric data have been used since the pharaohs, who certified their decrees with fingerprints. Pyramid construction workers were identified by name, physical size, face and foot shape, skin complexion, and scars. Obardat et al. (2019) mention that traditionally, biometrics applications focused on physical access control, such as controlling access to secure facilities or buildings using fingerprint scanners or facial recognition. Recent applications in physical security include integrity verification for passports.

Biometric data included in electronic passport documents—names, phone numbers, addresses, photographs, fingerprints, or any other identification data—represent a citizens' right to protection. Therefore, biometric data included in electronic passports guarantee the State and the individual sole control over information usage, preventing illicit use (CHEN, 2010).

Obardat et al. (2019) classify biometrics into three types: physiological, behavioral, and cognitive. Physiological biometrics include hand geometry, finger minutiae, and facial features. Behavioral traits encompass keystroke dynamics, mouse dynamics, gesture dynamics, signature dynamics, and voice. Finally, cognitive biometrics include emotional state. According to Frescura (2019), the term "biometrics" derives from the Greek "bios" (meaning life) and "metron" (meaning measure). These constitute important features for electronic passport identification, such as fingerprints, photographs, digital signatures, and iris recognition.

Thanks to biometric systems' development, data can be read in an automated manner. Data are currently classified into two categories: primary and secondary. Primary refers to the face stored on the chip, being the most current, while secondary includes fingerprints, iris recognition, and digital fingerprints. The main biometric data used in electronic passports are described below.

5.1 Facial recognition

Photography was not initially included in passports when states adopted them as documents after World War I but was incorporated in the 1920s with standardized

passports for international travel. While iris recognition technology appears to be a modern development, the concept dates back to 1936, when the iris was first proposed as a biometric trait (SANTI, 2017, p. 22).

According to Gipp et al. (2007), ICAO incorporated facial images into German electronic passports for the first time and soon perceived more advantages within other biometric data because it did not involve incorporating another type of information but simply displaying the face to the public. Thus, facial images are internationally accepted in identification documents.

In facial recognition, the system uses peaks, valleys, and contours within a face, treating these as nodes that can be measured and compared against those stored in the system's database, including jawline length, eye depth, distance between eyes, cheekbone shape, and nose width—approximately 80 nodes on a face. The human face is increasingly used for authentication purposes as a security system cue; the user is identified by comparing captured image data with data stored in the database (RAMYA et al., 2018).

Regarding biometric technology use, countries must consider their population's skin color when purchasing technological equipment. For people with black and Asian complexions, facial scanning can be more difficult to verify because devices are not always optimized to acquire darker faces (STENUM, 2017).

5.2 Fingerprints

According to Cortés et al. (2010), in 1880, Sir Francis Galton used fingerprints as personal identifiers, noting that fingerprints are made up of a series of dark lines representing ridges and a series of white spaces representing valleys, bifurcations, and ridge endings. Recognition of fingerprints in electronic passports to ensure they are unique must go through an analysis process consisting of several stages. First, the holder takes an impression on paper or metal plates using an electronic sensor. Then, algorithms are applied to improve image quality. Subsequently, pattern classification is identified, such as loops, arches, and whorls. In the feature extraction phase, so-called minutiae are located so that they are unique compared to others. Finally, the number of minutiae found and the degree of correlation are determined (GIPP et al., 2007).

Ezovski and Watkins (2007) mention that according to the scientific community, the National Institute of Standards and Technology (NIST) stated in 2002 that for greater superiority in fingerprint recognition, ten fingers would be required in biometric matters, with male fingerprints having better results due to larger fingers. Recognition quality varies by age: users under 20 years of age show better results, while those over 50 years of age show decreased recognition. Additionally, fingerprint recognition decreases depending on people's occupations; for example, a farmer compared to a businessperson. The same effects apply to iris recognition; it is not the same for a person in good health compared to a sick person.

Cortés et al. (2010) note that for fingerprint processing, One Touch for Windows SDK.NET Edition developed by DigitalPersona was used. This application is a software development tool that allows programmers to integrate fingerprint biometrics into a wide range of applications for the Windows operating system.

5.3 Iris recognition

Ramya et al. (2018) point out that iris recognition is a biometric identification method that involves recognizing the iris pattern of the eyes. The iris is a thin muscle in the eye that defines the diameter of eye color and pupil size.

The incorporation of the iris into electronic passports has been recent and offers advantages due to the fact that 250 unique characteristics can be identified in it, compared to fingerprints that have approximately 50 characteristics depending on image quality. In contrast to the advantages provided by iris recognition, the system to be used needs to be of high quality to meet users' needs, such as height and vision level (GIPP et al., 2007).

5.4 Digital signature

According to Cortés, Medina, and Muriel (2010), the digital signature is another less problematic biometric technique, representing very important data worldwide, and it is economical to implement. A system with a writing tablet connected to the computer is needed. The signature scan is analyzed from two points of view. The stored data include speed, pressure, direction, stroke length, and areas where the pen is lifted.

The digital signature is integrated into electronic passports to guarantee the integrity of other data. Additionally, through it, one can verify whether the data were issued by a legitimate authority and whether they have been manipulated by others. Through biometrics, the recognition of people occurs through sensory systems: vision, hearing, touch, taste, and smell, although the most common are vision and touch in electronic passports or other matters. However, biometric data have alterations in some aspects, both internal and external: aging, environmental impacts, databases, or social impacts.

The advantages provided by electronic passports include communication within and outside government. For governments, this influences greater responsiveness to citizens' needs and increases the coverage and quality of their services. It also improves the links between citizens and government, promoting greater interaction through information exchange (VARGAS, 2011).

6 CONCLUSION

Biometric technology is used to reliably verify individuals' identities. In the case of electronic passports, governments employ biometric systems for migration control, which contributes, among other aspects, to aviation security. It is important to note that biometrics is increasingly present in areas related to social control, such as security in both public and private institutions.

Several countries have transitioned from traditional passports to electronic passports due to incidents of identity theft and document forgery, leading to the implementation of biometric systems. The most common biometric data used in electronic passports include facial recognition, fingerprints, and iris recognition.

Moreover, effective management of biometric data and identity recognition technologies requires specialized technical knowledge, as these systems provide security to public and private institutions. In the context of electronic passports, their primary purpose is to offer citizens a secure identity document. However, biometric technology requires significant investment to deliver efficient services. In some cases, the biometric systems or technologies used by countries implementing electronic passports have exhibited vulnerabilities, resulting in identity theft. Therefore, governments must

continuously invest in and improve passport infrastructure to enhance security. While biometric technology has a positive impact on security, its effectiveness largely depends on the level of investment made. The primary beneficiaries of efficient biometric technology are users, who no longer need to remember passwords or codes and benefit from increased security and data privacy. For governments, a key outcome is the improved identification of terrorists and criminals.

Electronic passports must be regulated through international standards to ensure that identity documents are reliable and that services are secure at both national and international levels. Nevertheless, some issuing organizations provide these services without adequately considering that poor service quality can lead to identity fraud, as previously discussed. Social actors involved in passport-issuing organizations must have properly trained personnel capable of participating in the selection, design, and implementation of these systems in compliance with regulatory frameworks.

Finally, this topic opens avenues for future research, including in-depth analyses of biometric systems, privacy concerns, and smart borders, among others.

REFERENCES

BORDER PATROL OFFICE. National Border Patrol Strategy. U.S. Customs and Border Protection, 2004. Available from: http://www.cbp.gov.

CHEN, M. S. Privacidad y protección de datos: un análisis de legislación comparada. Costa Rica: Universidad de Costa Rica, 2010. Available from: http://www.redalvc.org/pdf/439/43915696004.pdf.

CORTÉS, O. J. A.; MEDINA, A. F. A.; MURIEL, E. J. A. Sistema de seguridad basada en biometría. Colombia: UTP, 2010. Available from: http://www.redalvc.org/articulo.oa?id=849209770016.

CÔTÉ-BOUCHER, K. The Diffuse Border: Intelligence-Sharing, Control and Confinement along Canada's Smart Border. Canada: Surveillance Studies Network, 2008. Available from: http://www.surveillance-and-society.org.

CRIADO, J. I.; ROJAS, M. F. Social Media and Public Administration in Spain: A Comparative Analysis of the Regional Level of Government. United States of America: CIDE, 2013. Available from: https://www.igi-global.com/.

DANKO, A. S.; FERNÁNDEZ, G. C. My Brain is My Passport. Verify Me. United States: International Conference on Consumer Electronics, 2016.

DÍAZ, M. G. A. Diseño y construcción de un modelo de política pública para implementar el pasaporte electrónico como herramienta para fortalecer la seguridad nacional. Un análisis del caso mexicano y sus retos en la acreditación de identidad. Monterrey: Tecnológico de Monterrey, 2014. Available from: https://repositorio.tec.mx.

DURAN, J. Virtual borders, data aliens, and bare bodies: Culture, securitization, and the biometric state. Journal of Borderlands Studies, 2010. DOI: http://dx.doi.org/10.1080/08865655.2010.9695785.

ENGELS, D.; FOLEY, J.; WALDROP, J.; SARMA, S.; BROCK, D. The Networked Physical World: An Automated Identification Architecture. Paper presented at the WIAPP - Second IEEE Workshop on Internet Applications, 2001.

ENTRUST. Soluciones de pasaportes electrónicos de Entrust. Estados Unidos, 2014. Available from: https://www.entrust.com/wp-content/uploads/2012/04/DS_Entrust-ePassport-Doc-Inspection_ESP_Sept2014.pdf.

EZOVSKI, G. M.; WATKINS, S. E. The Electronic Passport and the Future of Government-Issued RFID-Based Identification. USA: Missouri University of Science and Technology, 2007.

FOUCAULT, M. Seguridad, territorio, población: Curso en el Colegio de Francia 1977-1978. Buenos Aires: Fondo de Cultura Económica, 2014.

FRESCURA, T. D. E. Debates públicos en torno a la creación del Sistema Federal de Identificación Biométrica (SIBIOS): tensiones entre seguridad y privacidad. Argentina: Universidad de Buenos Aires, 2019. Available from: https://www.aucademica.org/000-023/410.

GIPP, B.; BEEL, J.; RÖSSLING, I. E-Passport: The World's New Electronic Passport. A Report about ePassport's Benefits, Risks and its Security. CreateSpace Independent Publishing Platform, 2007.

INTERNATIONAL CIVIL AVIATION ORGANIZATION (ICAO). Guide to Assessing Security in the Management and Issuance of Travel Documents. ICAO, 2010. Available from: https://www.icao.int.

MULLER, B. J. Risking it all at the Biometric Border: Mobility, Limits, and the Persistence of Securitisation. Geopolitics, 2011. Available from: http://dx.doi.org/10.1080/14650045.2010.493775.

OBARDAT, M.; TRAORE, I.; WOUNGONG, I. Biometric-Based Physical and Cybersecurity Systems. Springer, 2019.

PORWICK, P. The biometric passport. The technical requirements and possibilities of using. Poland: University of Silesia, 2009. Available from: https://www.researchgate.net/publication/224584311.

RAMYA, N.; SANDHYA, U.; GAYATHRI, L. Biometric Authentication to ensure security in ePassports. International Conference on Communication, Computing and Internet of Things (IC3IoT), 2018.

SANTI, P. S. E. Biometría y vigilancia social en Sudamérica: Argentina como laboratorio regional de control migratorio. México: UNAM, 2017. Available from: www.scielo.org.mx.

STENUM, H. The Body-Border. Governing Irregular Migration through Biometric Technology. Spheres: Philips, 2017. Available from: https://doi.org/10.25969/mediarep/3852.

VARGAS, H. J. G. Teoría Institucional y Neoinstitucional en la Administración Internacional de las Organizaciones. Argentina: UNM, 2011. Available from: https://www.redalyc.org/pdf/357/35779354710005.pdf.

WATKINS, S. E. The Electronic Passport and the Future of Government-Issued RFID-Based Identification. USA: Missouri University of Science and Technology, 2007.

YILDIZ, M. E-government research: Reviewing the literature, limitations, and ways forward. Turkey: HU, 2007.

Authors' Contribution

All authors contributed equally to the development of this article.

Data availability

All datasets relevant to this study's findings are fully available within the article.

How to cite this article (APA)

García, L. M. G., Pérez, V. A. G., García, S. J., Mendoza, S., Ahuactzi, J. C., & Silva, A. J. (2026). ELECTRONIC PASSPORTS: IMPORTANCE AND IMPLICATIONS. *Veredas Do Direito*, 23(4), e234853. https://doi.org/10.18623/rvd.v23.n4.4853