Kurdish Studies
Jan 2024
Volume: 12, No: 1, pp. 1057-1061
ISSN: 2051-4883 (Print) | ISSN 2051-4891 (Online)
www.KurdishStudies.net

Received: October 2023 Accepted: December 2023
DOI: https://doi.org/10.58262/ks.v12i1.071

Protection of Biometric Data When Using Filters on Social Networks
Protección De Datos Biométricos En El Uso De Filtros En Las Redes Sociales

Genesis Karolina Robles Zambrano[1], Manuel Augusto Suarez Albino[2] Ingrid Joselyne Diaz Basurto[3]

Abstract

The use of biometric data has facilitated access to many social networks and even banking applications. Facial recognition was first proposed more than 50 years ago, and today, the legal implications that its unauthorized use may carry are still being examined. The objective of this research is to determine the importance of protecting biometric data when using filters on social networks. The research falls within the qualitative approach and was developed in a documentary, descriptive type. The method used to conduct the research was the analytical-synthetic method. As one of the results, it is indicated that social networks, often without users even realizing it, have access to the internet protocol known as (IP), the image gallery, device location, language, and time, among others. Not to mention that when users access Facebook, Instagram, or TikTok, their interests, workplaces, income, and the people of interest are already determined through user actions. It is concluded that, in Ecuador, the Organic Data Protection Law classifies biometric data as sensitive information, meaning it is a special category of information that includes ethnic elements, health, genetic information, religious or moral beliefs, political affiliation, and even sexual orientation. Once violated, these data affect fundamental human rights, such as the right to privacy and intimacy.

Keywords: Protection, Biometric Data, Filters.

Resumen

La utilización de datos biométricos ha facilitado el acceso a muchas redes sociales, e incluso a las aplicaciones bancarias. El reconocimiento facial fue propuesto por primera vez hace más de 50 años y es hoy día en donde se analizan las implicaciones legales que el uso no autorizado del mismo pueda acarrear. Se plantea como objetivo determinar la importancia de la protección de datos biométricos en la utilización de filtros en las redes sociales. La investigación se enmarca en la modalidad u enfoque cualitativo y se desarrolló bajo el tipo documental, descriptiva. El método utilizado para realizar la investigación fue el método analítico-sintético. Como uno de los resultados se indica que las redes sociales, sin que los usuarios siquiera lo noten, tienen acceso al protocolo de internet conocido como (IP), la galería de imágenes, ubicación del dispositivo, idioma, hora entre otros. Esto sin contar que cuando se ingresa a Facebook, Instagram o TikTok, por acciones de los usuarios ya se determina cuáles son sus intereses, donde labora, cuáles son sus ingresos, quienes son sus personas de interés. Se concluye que, en el Ecuador, la Ley Orgánica de Protección de Datos cataloga los datos biométricos dentro de datos sensibles, es decir, es una categoría especial de información que indica elementos étnicos, de salud, de información genética, de creencias religiosas o morales, afinidad política e incluso preferencia sexual, que una vez violados, afectan un derecho humano fundamental como lo es el derecho a la intimidad y privacidad.

***Palabras Clave**: Protección, Datos Biométricos, Filtros,*

[1] Institution: Universidad Regional Autónoma de Los Andes, Extensión Quevedo-Ecuador. Email: uq.genesisrobles@uniandes.edu.ec, Orcid: https://orcid.org/0000-0002-2965-2091
[2] Institution: Universidad Regional Autónoma de Los Andes, Extensión Quevedo-Ecuador. Email: uq.manuelsa97@uniandes.edu.ec, Orcid: https://orcid.org/0000-0002-9257-273X
[3] Institution: Universidad Regional Autónoma de Los Andes, Extensión Quevedo-Ecuador. Email: uq.ingriddiaz@uniandes.edu.ec, Orcid: https://orcid.org/0000-0003-2934-4010

Introduction

For some years now, it has been a common feature that mobile phones no longer require numerical passwords for access, as well as some banking applications, which generally use facial recognition to grant user access.

Woodrow Bledsoe initially proposed facial recognition more than 50 years ago. This idea was a manifestation of his desire to see if computers could recognize human faces.

This initial idea presented by Woodrow Bledsoe, in the 1960s, intended to develop a system that could classify photos of faces using what is known as a RAND tablet. The idea was not successful since for it to work it was necessary to have very good lighting and stability in the image. This situation was often difficult since the author of this application demonstrated that the face or head has a lot of mobility and sometimes it was impossible to obtain a facial scanner.

After Bledsoe's idea, Goldstein, Harmon, and Lesk in 1970 were able to add greater precision to the initial concept, using specific markers that included lip thickness and hair color to automatically identify faces.

Already in 1988 Sirovich and Kirby began to apply linear algebra to the problem of facial recognition, and it worked as a search for a low-dimensional representation of facial characters. Sirovich and Kirby were able to demonstrate that analyzing features on a collection of facial images could form a set of basic features. (Bello Janeiro, 2020)

It was in the 1990s when the Defense Advanced Research Projects Agency (DARPA) and the National Institute of Standards and Technology launched the Facial Recognition Technology (FERET) program, initiating the promotion of the use of facial recognition within the commercial market.

According to Montes de Oca Suarez (2023), "It was from 2010 that Facebook began to implement facial recognition functionality that helped identify people whose faces may appear in the photos that Facebook users update daily".

Nowadays, facial recognition is so common that it can be found in airports, and social networks through the use of filters and the use of photos, and bank applications, among others. But it is worth asking ourselves, who and why have access to all that biometric information that is generated every time a facial recognition is performed, and if it is also possible to protect that data. (Garriga Domínguez, 2016)

Now, when talking about facial recognition, biometric data has to be mentioned. According to Jain, Ross, and Pankanti (2000): "Facial recognition is the process of identifying or verifying the identity of an individual using their unique facial characteristics", and this is possible thanks to biometric data.

In his book "Biometric Recognition: Challenges and Opportunities" (2010), Anil K. Jain defines it as: "The identification of a person from an image or sequence of images of his or her face".

On the other hand, in the book "Introduction to Biometrics" by Anil K. Jain, Arun Ross, and Karthik Nandakumar (2011), biometric data is defined as follows: "Biometric data are numerical measurements or symbolic representations of physiological characteristics or behavioral patterns unique to an individual, which are used to establish or verify their identity.

According to the "Biometrics Identity Management Agency" report of the National Institute of Standards and Technology (NIST) of the United States, biometric data is defined as: "Physical or behavioral characteristics intrinsic to an individual, which can be used to establish or verify his identity uniquely and reliably.

As mentioned above, facial recognition and biometric data are closely related since facial recognition is a biometric identification method, which aims to collect unique and distinctive characteristics of an individual that can be used for identification or verification of their identity. (Lee-Morrison, 2019)

As mentioned previously, Facebook began using this technology in 2010, only with images. The application

automatically recognized the faces of the people who were in the photos and generated suggestions so that they could be tagged.

As stated, it was done automatically without the need for prior authorization, which in some way affects the right to privacy, but at that time not many legal reflections were made since no objection was presented except for a class action lawsuit in Illinois, United States. This conflict took place over several years, ending in a reform or update of the social network, where prior authorization of facial recognition is necessary, in addition to a million-dollar fine imposed by the Court Supreme on Facebook.

But what happens with the filters that users use on Instagram, TikTok, or other social networks? Applying filters requires facial recognition so that the filters can be applied. Therefore, if they are used without the user's prior authorization, biometric data would be provided without legal authorization from the "owner". That is, they would be using features, characteristics, and any information of the individual without authorization. (Upegui Mejía, 2020)

Based on the information described above, the general objective of this article is to determine the importance of the protection of biometric data in the use of filters in social networks, since as explained at the beginning, when using the filters of these networks a series of user data that could have not been authorized by them is collected.

Methodology

The article falls within the qualitative modality or approach, which, as defined by Sampieri, aims to describe, understand, and interpret phenomena through the perceptions and meanings generated by the experiences of the participants. (Sampieri, 2014).

Other authors such as Hernández, Fernández, and Baptista (2010) state that the qualitative approach uses data collection without numerical measurement to discover or refine research questions during the interpretation process.

In this sense, this paper aimed to use documentary information that allowed the description of a phenomenon within the legal context to analyze its legal implications.

Furthermore, the research was conducted under the documentary and descriptive type, which is defined by Tamayo (1994) as "the record, analysis, and interpretation of the current nature and composition or processes of phenomena".

The method used to carry out the research was the synthetic analytical method, which refers to two inverse processes that operate in a single unit, that is, analysis and synthesis. (Rodriguez and Perez, 2017)

Results

According to the United Nations Compendium of Best Practices for the Responsible and shared use of biometrics in the fight against terrorism, biometrics is a useful and functional tool to combat terrorism. It can prevent terrorist actions and protect society.

On the other hand, the United Nations has stated that biometric technology uses and stores data that is mostly of a personal nature. These data must be protected and safeguarded in states through regulations to ensure they do not violate a fundamental human right, such as the right to privacy.

Based on the lawsuit filed by the state of Illinois against the social network Facebook, it was demonstrated that it had collected biometric data protected by its Instagram users and in this way reinforced facial recognition in all its products, thus violating the right to privacy. (Zhang et al., 2006)

Social networks, without users even noticing, have access to the Internet Protocol known as (IP), the image gallery, device location, language, and time, among others. This is not to mention that when a user accesses Facebook, Instagram, or TikTok, the actions of the user generate information about what their interests are, where they work, what their income is, and who their people of interest are.

In the case of the social network TikTok, in 2021 it expressed a change and update to its terms of use and

conditions, which expressed the collection of biometric data in the protagonists of its videos, a situation that generated a great impact among its users since there is no way to avoid accepting said condition since it is a *sine quanon* requirement to be able to access the app.

The ISO/IEC TR 24741:2018 standard, from the International Organization for Standardization (ISO), defines biometric data as the automatic recognition of individuals based on their biological and behavioral characteristics.

In turn, the Organic Law on the Protection of Personal Data (LODPDP) defines biometric data as unique personal data related to the physical or physiological characteristics or even the behaviors of a natural person that allows or confirms the unique identification of that person, such as facial images or fingerprint data, among others.

One of the benefits that the use of biometric data on social networks would entail would be the verification of the age of the users of the networks before accessing them, to limit their use to minors and thus protect them in the future from cyber criminals, or identity theft. As is the case of Instagram, which has implemented this biometric recognition software to identify that the person is of the appropriate age to create a profile. (Tapiador Mateos & Colas Pasamontes, 2005)

Discussion of Results

While it is true that the use of biometric technology can support the eradication of terrorism, its indiscriminate use can lead to a certain margin of error. For example, in Brazil, due to algorithmic bias, hundreds of individuals detained through the use of facial recognition have been predominantly black, as there is around a 10% margin of error.

In the United States, biometric and facial recognition technology is used in border areas to compare with visas and passports. The mere fact that this practice is carried out involves the analysis of all individuals' faces, regardless of whether they have a criminal record or are suspected of a crime.

Based on the definition of biometric data in Ecuador's Organic Law on the Protection of Personal Data, as stated in Article 4, it can be inferred that the data collected by such software must be capable of uniquely identifying an individual. Therefore, it may be necessary to validate that identity by cross-referencing it with a database, which in the case of Ecuador could be the Civil Registry. This means that the personal information of individuals would be accessed.

In the specific case of the use of social media, facial features are being collected through the use of filters. To adapt a filter to the shape of the face, software is required. In applications like TikTok, there is no prior consent from the social media user to authorize the collection of biometric data, as automatically using the app implies "tacit acceptance of the terms and conditions." Users may not be fully aware of the legal implications.

As mentioned in the results, there may be benefits to using biometric data recognition to determine the age of users and protect children from using social media. However, for individuals who use filters indiscriminately, it should be clear that these filters collect biometric data that could be used for deepfakes. Deepfakes are files or videos manipulated through artificial intelligence to make them appear original or authentic.

Conclusions

It is concluded that the collection of biometric data serves for the verification of the identity of one or more individuals. Therefore, it is necessary to cross-reference this data with a national or international database that corresponds to the collected information.

In Ecuador, the Organic Law on the Protection of Data categorizes biometric data as sensitive information. This means it falls into a special category of information that includes ethnic elements, health information, genetic data, religious or moral beliefs, political affiliations, and even sexual orientations. Once violated, these data can impact a fundamental human right, namely, the right to privacy and intimacy. They are categorized as sensitive because no one can be forced to provide them.

The term "deepfake" first appeared in the 1990s but gained significant attention in 2017. The term consists of two words:

"deep (learning)", which refers to automated processes with artificial intelligence, and "fake," which means false. It is used to deceive users into believing that images, videos, or the individuals featured in them are real. All of this is done using biometric data collected through facial recognition, often via various applications, especially on social media.

References

Bello Janeiro, D. (Ed.). (2020). *Nuevas tecnologías y responsabilidad civil* (1.a edición). Editorial Reus.

Garriga Domínguez, A. (2016). *Nuevos retos para la protección de datos personales: En la Era del Big Data y de la computación ubicua*. Dykinson.

Lee-Morrison, L. (2019). *Portraits of automated facial recognition: On machinic ways of seeing the face*. transcript.

Montesdeoca Suárez, A. (2023). *Intimidad y protección de datos personales en un contexto de trabajo digital*. Aranzadi.

Tapiador Mateos, M., & Colas Pasamontes, J. (Eds.). (2005). *Tecnologías biométricas aplicadas a la seguridad*. RA-MA.

Upegui Mejía, J. C. (2020). *Transparencia estatal y datos personales: El problema de la publicidad de la información personal en poder del Estado: estudio comparado México-Colombia* (Primera edición). Universidad Externado de Colombia.

Zhang, D., Jing, X., & Yang, J. (2006). *Biometric image discrimination technologies*. Idea Group Pub.

Rodríguez, A. y Pérez, A. O. (2017). Métodos científicos de indagación y de construcción del conocimiento Revista EAN, 82, pp.179-200. https://doi.org/10.21158/01208160.n82.2017.1647