INFORME SOBRE ASPECTOS BIOÉTICOS, LEGALES Y PROCESALES

del derecho a la identidad y el uso de procedimientos de reconocimiento facial por las fuerzas y cuerpos de seguridad

Paulo Ramón Suárez Xavier

COLEX

COLEX READER

UNIVERSIDAD DE MÁLAGA

GOBIERNO DE ESPAÑA MINISTERIO DE UNIVERSIDADES

Plan de Recuperación, Transformación y Resiliencia

Financiado por la Unión Europea NextGenerationEU

¡Gracias por confiar en Colex!

La obra que acaba de adquirir incluye de forma gratuita la versión electrónica.
Acceda a nuestra página web para aprovechar todas las funcionalidades de las que dispone en nuestro lector.

Funcionalidades eBook

Acceso desde cualquier dispositivo

Idéntica visualización a la edición de papel

Navegación intuitiva

Tamaño del texto adaptable

Puede descargar la APP "Editorial Colex" para acceder a sus libros y a todos los códigos básicos actualizados.

Síguenos en:

INFORME SOBRE ASPECTOS BIOÉTICOS, LEGALES Y PROCESALES DEL DERECHO A LA IDENTIDAD Y EL USO DE PROCEDIMIENTOS DE RECONOCIMIENTO FACIAL POR LAS FUERZAS Y CUERPOS DE SEGURIDAD

REPORT ON BIOETHICAL, LEGAL AND PROCEDURAL ASPECTS OF THE RIGHT TO IDENTITY AND THE USE OF FACIAL RECOGNITION PROCEDURES BY SECURITY FORCES AND BODIES

Calle Costa Rica, número 5, 3.º B (local comercial)
A Coruña, C.P. 15004
info@colex.es
www.colex.es

INFORME SOBRE ASPECTOS BIOÉTICOS, LEGALES Y PROCESALES DEL DERECHO A LA IDENTIDAD Y EL USO DE PROCEDIMIENTOS DE RECONOCIMIENTO FACIAL POR LAS FUERZAS Y CUERPOS DE SEGURIDAD

REPORT ON BIOETHICAL, LEGAL AND PROCEDURAL ASPECTS OF THE RIGHT TO IDENTITY AND THE USE OF FACIAL RECOGNITION PROCEDURES BY SECURITY FORCES AND BODIES

Paulo Ramón Suárez Xavier

COLEX 2023

Sumario

BERICHT ÜBER BIOETHISCHE, RECHTLICHE UND VERFAHRENSASPEKTE DES RECHTS AUF IDENTITÄT UND DIE VERWENDUNG VON GESICHTSERKENNUNGSVERFAHREN DURCH SICHERHEITSKRÄFTE UND -ORGANE

INFORME SOBRE ASPECTOS BIOÉTICOS, LEGALES Y PROCESALES DEL DERECHO A LA IDENTIDAD Y EL USO DE PROCEDIMIENTOS DE RECONOCIMIENTO FACIAL POR LAS FUERZAS Y CUERPOS DE SEGURIDAD

PRESENTACIÓN

El presente informe se realiza en virtud del proyecto de investigación individual «Inteligencia artificial, policía predictiva, reconocimiento facial y garantías procesales en un Estado de Derecho», que ha obtenido una de las Ayudas Margarita Salas para Jóvenes Doctores y que, entre otros objetivos, preveía la elaboración de un informe sobre el uso de datos faciales en técnicas de policía predictiva, especialmente, las técnicas de reconocimiento facial.

La realización del presente informe culmina una serie de estudios y publicaciones realizados en los últimos quince meses en dos estancias posdoctorales, la primera en la Universidad de Barcelona, en el ámbito del Observatorio de Bioética y Derecho de la Universidad de Barcelona, bajo la supervisión de las Dras. Casado González y de Lecuona Ramírez, a quienes no tenemos más que palabras de agradecimiento por todo lo compartido.

Por otro lado, y en referencia a la segunda estancia de investigación, realizada en el Centro para las Tecnologías de la Información y Propiedad Intelectual (CITIP) de la Facultad de Criminología y Derecho de la Universidad de Lovaina, bajo la supervisión de la Dra. Marie-Christine Janssens, Directora del Centro, tampoco podemos dejar de expresar nuestra gratitud, visto que las consultas realizadas en el CITIP han sido esenciales para la consolidación de las conclusiones llevadas a efecto en el presente informe.

Súmense, además, en los agradecimientos que integran la presentación de este informe, nuestras palabras de gratitud hacia el Área de Derecho Procesal de la Universidad de Málaga, especialmente a la Dra. Fontestad Portalés, que además de valiosos consejos y apoyo a lo largo de este proyecto y estancia, ha aceptado noblemente el encargo de supervisar

institucionalmente la presente investigación, desde la Universidad de Málaga.

Por fin, pero no menos importante, nuestro agradecimiento a las instituciones que apoyan y financian la presente investigación, entre las que quisiéramos mencionar la Universidad de Málaga, el Ministerio de Universidades y la Unión Europea, que financia la presente investigación con los Fondos Next Generation, a través del Plan de Recuperación, Transformación y Resiliencia.

En este sentido, lo primero que podemos afirmar sobre el presente informe, es que nace de la colaboración institucional de tres diferentes centros, apoyando la investigación desarrollada por su autor a lo largo de los últimos quince meses.

Algunas ideas, como el concepto de policía predictiva, la normativa incidente en el procedimiento de identificación, las bases de datos que se están creando a nivel europeo y algunas de las cuestiones que se tratan de forma resumida en el presente informe, fueron adecuadamente tratadas en las diferentes investigaciones publicadas en el período de la estancia, entre las cuales, señalamos la obra *Policía predictiva: entre seguridad y garantías procesales*, publicada por la Editorial Colex en 2022.

Sin embargo, y tal y como ya se va incorporando en la práctica de investigación, la academia debe, además de investigar y publicar los estudios que se realizan en los distintos proyectos llevados a cabo, acercarse e intentar solventar problemáticas sociales, jurídicas y políticas que emergen de los fenómenos estudiados.

Por ello, y como resultado de difusión del proyecto de investigación «Inteligencia artificial, policía predictiva, reconocimiento facial y garantías procesales en un Estado de Derecho», hemos realizado el presente informe, que tiene por objetivo exponer las problemáticas fundamentales generadas por el reconocimiento facial como técnica de policía predictiva, además de exponer una serie de recomendaciones relacionadas con tales problemáticas.

Esperamos que estas páginas puedan inspirar reflexión por parte de la sociedad civil, de los gestores y autoridades públicas y, como no podría dejar de ser, de la comunidad científica nacional e internacional, por lo que agradecemos

al apoyo de Boris Perisic en la traducción al inglés, alemán y francés.

En Barcelona, 09 de febrero de 2023,

Dr. Paulo Ramón Suárez Xavier
Investigador posdoctoral «Margarita Salas»
Observatorio de Bioética y Derecho de la Universidad de Barcelona
Área de Derecho Procesal – Universidad de Málaga

REPORT ON BIOETHICAL, LEGAL AND PROCEDURAL ASPECTS OF THE RIGHT TO IDENTITY AND THE USE OF FACIAL RECOGNITION PROCEDURES BY SECURITY FORCES AND BODIES

Paulo Ramon Suarez Xavier
Postdoctoral Researcher Margarita Salas
University of Malaga – University of Barcelona
Bioethics and Law Observatory

STATE OF THE ISSUE

1. Perspective of identification procedures through biological characteristics

Since the advancement of technologies related to the identification of people by genetic profiles, that is, by means of DNA tests, the way of identifying people before the state authorities in an administrative and/or judicial procedure has been profoundly altered.

Already at that initial moment of the advancement of biotechnology and nanotechnologies, at least in what refers to the clear affectation of the fundamental rights of citizens, the Bioethics and Law Observatory of the University of Barcelona has adopted a position regarding the need to safeguard the rights related to personal and family privacy.

Although, at that time, the overview that was presented and the core of fundamental rights affected by identification procedures based on DNA profiles was restricted to less complex issues, such as the protection of children and the validity of tests carried out outside a judicial procedure in the alteration of paternity, the advance of new technologies and big data have highlighted the need to delve into various aspects, including the reuse for exploitation purposes of the health data of users of the health system public, an issue also addressed by the Law and Bioethics Observatory in a 2015 document.

However, if we focus on these different but overlapping issues, we will realize that one of the central elements of the discussions that are revealed with the use of health and genetic data refers to the identification of people and to which we have agreed to call «identity».

Identity can be defined in different ways, all correct, as a set of characters that make a certain individual unique in the community. So it is possible to speak, more than identity, of identities, taking into account the wide spectrum of possibilities of individualization of a person.

In this sense, the advancement of technology has allowed the adoption of new person identification procedures through patterns, such as fingerprint recognition, iris recognition and, more recently, facial recognition.

These identification procedures reveal some complex issues. The first of these refers to the constitution of databases containing biological and biometric data of citizens, both in the public and private spheres, evidencing the disparity in protection between these and DNA, whose constitution of databases is restricted to some very specific assumptions established by Organic Law 10/2007, of October 8, regulating the police database on identifiers obtained from DNA and the seventeenth additional provision of Organic Law 03/2018, of December 5, Protection of Personal Data and guarantee of digital rights.

In the case of the constitution of databases with biometric data information, including facial images, iris data, fingerprints and other biometric profiles, there are a series of issues that deserve to be highlighted, since they refer to the same need for protection of the fundamental rights of

citizens, indicated in the different reports prepared by the OBD in the two decades.

2. Right to identity and identification

If there are different processes and procedures for the identification of people and, for the most part, they use the creation of biometric, biological, health and genetic databases, to what extent can their use affect the fundamental rights of citizens? What rights can be affected by these measures?

To answer this question, which is of vital importance for this document, we must resort to a right implicit in international treaties, but explicitly declared by the Spanish Constitution: the right to identity, translated by the constituent into the right to one's own image., guaranteed by the Spanish Constitution in its article 18, section 1.

The identity, the image that a subject holds in front of a social group and in front of himself is an essential element for the free development of the personality. The image, the face, an essential element of the subject's identity is the indelible reflection of the personality that nature and the human condition itself bestows on a member of a family, of society.

In this sense, the constituent has granted special protection to the image, to personal intimacy, to ideological and religious freedom and, ultimately, to the dignity of the person and the free development of the personality, which are, it says the constituent, foundation of political order and social peace.

The image defines individual identity and is a vital part of it. Socially, it is the way in which people identify with each other in society, family and institutions and, legally, it is the primary way of identifying citizens before public authorities.

The right to identity and to one's own image is very personal and, therefore, subjects are allowed to influence, even in an invasive way, their own image, changing it through different forms of action, through surgical and non-surgical procedures, natural or through the use of resources capable of altering, according to the will of its owner, the characteristics of its image.

This right cannot and should not be limited by issues related to the operation of identification procedures. This is because identity is not confused with identification. The first is a fundamental right, while the second is an obligation of the State that can be met from different perspectives and under the principles of equal treatment and non-discrimination, opportunity, proportionality, effectiveness, efficiency and responsibility.

Equal treatment implies that identification procedures must not generate any inequality in relation to sex, origin, social orientation, sexual orientation or any other form of discrimination.

The opportunity implies that the identification procedure must have a legal basis. In other words, it must be aimed at fulfilling the legal purposes established for it, which are the prevention of the commission of crimes and the identification of suspects, or to identify those responsible for administrative offenses when, in view of the circumstances concurrent is considered necessary by the security forces and bodies.

Proportionality refers to the means, implying the need to use the identification measure that is less burdensome for the citizen who submits to said procedure, which implies that the use of ostensive automated identification procedures would have no protection. in our legal system and in our human rights protection system.

Effectiveness and efficiency refer to resources and actions. A procedure is effective when it correctly serves the established purposes, causing no damage or causing the least possible damage (proportionality), to which is added the need for efficiency, that is, to carry out said purpose with the least possible waste of resources.

Although they are important, these principles cannot overcome the full effectiveness of fundamental rights and this is established in article 4 of Organic Law 04/2015, section 1, by reaffirming the need to observe the fundamental rights of citizens in actions for the maintenance and restoration of citizen security and the special powers of the administrative security police.

In other words, the actions related to identification capable of undermining the right to identity guaranteed by the Spanish Constitution and the international treaties to which Spain is a

party, as well as the international treaties that guarantee the right to human dignity, contradict the logic of protection of fundamental rights, stripping the subject of his own identity, his own image, to the extent that the limitations imposed exceed what is strictly necessary for the maintenance of public order.

It is the duty of the State to respect the identity and at the same time identify citizens for the exercise of their rights and for the maintenance of order and social peace, in order to protect the right to self-image of citizens, as well as the right to the protection of personal data.

3. Protection of personal data and identification

Identification procedures, especially facial recognition processes through image and sound capture systems on public roads, undermine not only the right to one's own image and the right to identity, but also the right to personal data protection.

The protection of personal data of citizens had its first international recognition with the Convention for the protection of persons with respect to the automated processing of personal data, made in Strasbourg on January 28, 1981, which recognizes as a of the exceptions to the general limitation for the processing of personal data without due guarantees the regime for the protection of State security and public security.

Along the same lines, article 8 of the Charter of Fundamental Rights of the European Union defines the right to the protection of personal data as one of the fundamental freedoms within the European Union, an understanding to which is added the Article 8 of the European Convention on Human Rights, by limiting the possibility of public authorities to interfere in the exercise of these rights, except as strictly necessary to guarantee national security, public safety, the economic well-being of the country, defense of order and the prevention of criminal offences, the protection of health or morals, or the protection of the rights and freedoms of others.

Data protection, in this sense, constitutes a right-tool, with a view to guaranteeing personal and family privacy and the identity of individuals against undue interference in their individual and family spectrum, hence rectification, cancellation and consultation as fundamental aspects for its exercise.

In other words, the personal data of an individual constitute, from a bioethical perspective defended by the Bioethics and Law Observatory, an essential part of the subject's condition as a person in the digital society, allowing them to freely integrate into the network as a member of society, with due control that strictly authorized use will be made of their personal information.

This idea, which is opening space to concepts such as self-sovereign digital identity, in which the individual has total and absolute control over the use of their personal data, as if it were a single window, whose objective is to replace the already obsolete notice and choice model currently incorporated in our legislation.

The fundamental issue refers to the fact that the Organic Law on Data Protection and the European Data Protection Regulation have excluded from their scope of application the processing of data for the purposes of prevention, investigation, detection or prosecution of criminal offences, or enforcement of criminal sanctions, including protection against threats to public security and their prevention.

A) EU Directive 680/2016, regarding the protection of natural persons with regard to the processing of personal data by the competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offenses or the execution of sanctions and the free circulation of such data

In these areas, which includes the protection of public security, the provisions of EU Directive 680/2016 are applied, regarding the protection of natural persons with regard to the processing of personal data by the authorities. competent authorities for purposes of prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal sanctions, and the free circulation of said data.

In its article 3, the Directive defines biometric data as those personal data obtained from a specific technical

treatment, related to the physical, physiological or behavioral characteristics of a natural person that allow or confirm the unique identification of said person, such as images facial or fingerprint data.

Biometric data constitute, as established in article 10 of the Directive, the group of special category data, permitted exclusively when strictly necessary, subject to adequate safeguards for the rights and freedoms of the interested party and only when authorized. the Law of the Union or of the Member State; is necessary to protect the vital interests of the interested party or of another natural person, or when said treatment refers to data that the interested party has made manifestly public.

Curiously, although it mentions video surveillance in Recital 26, the Directive does not explicitly authorize the use of facial recognition techniques or the use of video surveillance cameras that process personal data live by means of mobile or fixed equipment.

The video surveillance to which the Directive refers in its recitals is not video surveillance by means of equipment that allows facial recognition, but the use of cameras to record the events that take place on public roads and whose regulation in Spain was given by Organic Law 04/1997, of August 4, which regulates the use of video cameras by the Security Forces and Bodies in public places.

On the other hand, with regard to its nature, it should be noted that EU Directive 680/2016 constitutes a Directive of minimums, which implies that the Member States can expand the range of guarantees contained in its text, but not restrict them, which leads us to the need to examine the legislative text that results from its transposition.

B) Organic Law 7/2021, of May 26, on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal offenses and the execution of criminal sanctions

The Organic Law 7/20221, of May 26, transposes the EU Directive 680/2016 to our legal system, although it marks distances in a series of issues related to the issues related to the processing of biometric data, since it goes far beyond the provisions of the European standard.

Indeed, unlike the Directive, which only exceptionally authorizes the use of biometric data, the Organic Law authorizes the processing of biometric data to uniquely identify a person, a category in which facial recognition is included, without further ado. requirements, which implies a serious restriction of the exceptional regime defined by article 10 of EU Directive 690/2016.

To make the use of these technologies viable, article 15 of Organic Law 7/2021, of May 26, authorizes the capture of image and sound by security forces and bodies on public roads, with a view to allowing data processing. biometric devices, without specifying the authorization system for these devices, as recommended by Organic Law 04/1997.

Said generic authorization, which also excludes the processing of biometric data for purposes of identification within the scope of the right to honour, personal and family privacy and one's own image, for the purposes of the provisions of article 2.2 of Organic Law 1 /1982, constitutes a clear violation of the provisions of article 18, sections 1 and 4 of the Spanish Constitution.

It should be noted that the use of biometric data of citizens should be exceptional and strictly applied to meet specific needs, when a higher public interest is at stake, without this implying an automatic presumption of this interest in any action of the forces and bodies of security.

This broad authorization implies, additionally, in a clear violation of the Fundamental Rights proclaimed in the Charter of Fundamental Rights of the European Union, which in its articles 7 and 8, which define the rights to the protection of private and family life and the right to data protection and its control by an independent authority.

Said authority, in the case of Organic Law 7/2021, of May 26, does not correspond to the concept of independent authority, since it falls on cases of treatment by the Public Prosecutor's Office in the Public Prosecutor's Office itself and in the Council General of the Judicial Power in the cases of procedural actions and in various bodies in the case of the Security Forces and Bodies, which implies a diffuse regime and little security for the owners of the data processed.

This regime generates concern on the part of the Bioethics and Law Observatory, which sees a series of risks to human

dignity, bioethical problems related to the manipulation of information, the violation of the right to freedom and the free development of the personality of groups vulnerable and minorities, as well as its possible use for undesirable purposes by third states that receive this information.

Such considerations and the inadequate transposition of the EU Directive 680/2016 by the Spanish Legislator, by introducing significant changes in the biometric data processing regime, altering the dynamics of maximum harmonization adopted by the Directive, demand an active position on the part of institutions and civil society, in defense of fundamental rights.

C) The position of the Ombudsman regarding the Constitutionality of Organic Law 7/2021, of May 26

As stated in the annual report of the Ombudsman for the year 2021, the high commissioner of the Cortes Generales has received a citizen request to present an appeal of unconstitutionality against articles 5, 9, 15, 17 and 24 of the Organic Law 7 /2021, whose examination is found in said report.

In it, the Ombudsman highlights that the regulation established by EU Directive 680/2016 is comparable to that regulated by EU Directive 681/2016, regarding the Passenger Name Registry, since both are determined by the same purpose to prevent, investigate and prosecute crimes.

Remember, citing the doctrine of the Constitutional Court, that the protection of privacy and the protection of personal data is not absolute and may be limited by a constitutionally relevant reason, capable of authorizing the restriction of these rights to the extent necessary for the achievement of these ends.

It concludes, after an examination of the proportionality, legality of the objective and the model of guarantees established (basically a system of pecuniary compensation and fines), on the constitutionality of the regulation established by Organic Law 7/2021, deciding not to file an appeal. unconstitutionality.

The position of the High Commissioner of the General Courts regarding such a sensitive issue causes great concern to the Bioethics and Law Observatory and to the signatories of this document, considering, among many other aspects,

that the processing of biometric data cannot be equated to Registration of Passenger Names, since in this case we are dealing with the most elementary identification data of the subject, without this being related to an invasion of privacy and image.

Secondly, especially in relation to the provisions of section 2 of article 13 of Organic Law 7/2021, it does not establish a guarantee regime, but instead authorizes in an unrestricted manner the possibility of processing biometric data by the competent authorities, which implies an authorization for the processing of this data even for those people who are not suspected or have been convicted of any crime.

Thirdly, although it is true that there are no absolute rights, the restriction of fundamental rights of such importance as the right to one's own image, to data protection and to personal and family privacy in a Rule of Law depends on a system of guarantees that allow citizens to glimpse that these limitations are a justified exception, not the rule, an aspect clearly ignored in the regulation established by article 13, section 2 and by articles 15, 16 and 17 of the Organic Law 7/ 2021.

Finally, regarding the system of guarantees, it is of concern to consider that the disciplinary system established by article 19 of Organic Law 7/2021 and by the rights to compensation provided for in articles 53 (treatment by public entities) and 54 (treatment by private entities), are sufficient to protect the fundamental rights of citizens against technologies that are proven to be subject to errors and whose effects on the lives of citizens can be disastrous at all levels.

The Observatory of Bioethics and Law and other signatories of this document recall that Freedom is a higher value in the Spanish Constitution. It is not by chance that freedom is mentioned before justice in article 1, since justice without freedom is oppression and freedom without justice is anarchy.

Freedom must prevail in our legal system, which is part of the European Space of freedom, security and justice, in which the same observation mentioned above applies, so we invite the High Commissioner of the Cortes Generales to review his position regarding the constitutionality of the aforementioned provisions of Organic Law 7/2021, whose content clearly violates the fundamental rights established

in article 18, sections 1 and 4, as well as data protection and the right to free development of personality.

This position echoes the recent demonstrations of the European Parliament approved by means of the Resolution of October 06, 2021, on intelligence

in criminal law and its use by police and judicial authorities in criminal matters (2020/2016(INI)), which calls for the permanent prohibition of the use of other human characteristics in spaces accessible to the public, such as walking, fingerprints, DNA, voice and other biometric and behavioral signals.

Freedom is always the starting point of the proposals of the Opinion Group of the Bioethics and Law Observatory, from which the limits and the possibility of restricting the exercise of fundamental rights are established. The restriction cannot and should not be the measure of freedom, but its exception, based on the law and protected by a court ruling when the entity of the restriction so requires, as is the case with the use of information technologies. facial recognition.

STATEMENT

STATEMENT OF MOTIVES

Taking into account that:

- Biometric data is particularly sensitive data and its inappropriate use and treatment can generate a series of violations of Fundamental Rights;
- The absence of an established framework regarding the reuse of biometric data by companies and by public administrations, especially of deceased persons;
- Facial recognition systems are biased and their use by the State in criminal matters can affect various social minorities;
- Predictive systems can make correlations between data sets, but cannot establish causal relationships or reliably predict human behavior,
- The identification of the citizen as a duty and right should not undermine their fundamental right to identity;
- The operation of facial recognition algorithms may require limitations on the use of accessories, makeup, veils, and other aspects of the image and identity of citizens;

Taking into account that:

- The transposition of EU Directive 680/2016 has not provided for an independent authority to control the processing of personal data in criminal matters, but rather has entrusted said powers to the police authorities, the Public Prosecutor's Office and the General Council of the Judiciary;
- The processing of biometric data on public roads by fixed and mobile systems, in real time or deferred, violates the presumption of innocence and the right to identity of citizens who are not suspected of having committed crimes and restricts their freedom;
- The operation of facial recognition algorithms may require limitations on the use of accessories, makeup,

veils, and other aspects of the image and identity of citizens, limiting their right to the free development of personality;
- The performance of aesthetic procedures can easily circumvent the operation of facial recognition technologies and prevent their operation;
- The risks that a false coincidence may generate for the citizen who is confused with a person suspected or convicted of a crime;
- The lack of clarity regarding the requirements and the way of carrying out the identification procedure.
- The Researcher of the Bioethics and Law Observatory has reached the following

CONCLUSIONS

I – The use of facial recognition technologies, pattern recognition and other algorithmic techniques aimed at identifying people should not be used conspicuously on public roads, since it offers a series of risks to freedom, identity and citizen privacy.

Its use must be restricted to cases of necessity and there must be judicial authorization for it. Otherwise, the superior value of freedom and related fundamental rights would be flagrantly violated.

II – The use of facial recognition technologies in identification procedures can generate serious violations of the fundamental right to the free development of the personality and the fundamental right to identity, therefore the necessary actions to guarantee its correct operation, such as the obligation of wearing a bare face, the prohibition of the use of hyper-realistic masks or certain types of makeup, would end up causing more damage than the use of other technologies capable of guaranteeing citizen security.

It is recommended that its use, in the event that it is carried out, be done in such a way as to protect the legitimate exercise of fundamental rights, such as identity and the free development of the personality, without any discrimination, including religious discrimination.

III – The control system for the use made of personal data in criminal matters, including biometric data, must be subject to the control of an independent authority, as established in article 8 section 3 of the Bill of Rights Fundamentals of the European Union. The concept of control authority defined by EU Directive 680/2016 and the transposition carried out by Organic Law 7/2021 contradict this precept.

It is recommended that changes be made to Organic Law 7/2021, for the inclusion of an independent authority instead of the currently planned control authorities and self-regulation system.

IV – In relation to the formation of databases containing biometric images of all citizens, promoted by EU Regulation 2019/1157 in its article 3, section 5, and article 10. Its use and treatment must comply with guarantee standards, avoiding

the transfer of this data to third countries in which there is no system of legal guarantees of its use and reuse.

It is recommended that the commercial use that can be made of this data be limited, especially with a view to avoiding its reuse for the creation of machines and software whose interface includes a human face without the authorization of the owner of the image.

V – With regard to the use of fixed and mobile image and sound recording devices on public roads, with the possibility of processing personal and biometric data in real time or deferred, it is recommended that their conspicuous use be prohibited, conditioning the justified use that is mentioned in the first conclusion to its authorization by means of a motivated judicial decision and duly directed to the data protection authority.

In this sense, it is recommended to review the structure of the procedure established in articles 15, 16 and 17 of Organic Law 7/2021.

VI – The current configuration of the data protection system in criminal matters, established by Organic Law 7/2021, violates a series of Fundamental Rights, for which it is recommended that the legitimate authorities file an appeal of unconstitutionality, that is, Deputies (50), Senators (50) to adopt said measure, especially in relation to the unrestricted authorization for the use of constant facial recognition in article 13, section 2.

The Ombudsman is recommended to review the understanding declined in the decision not to file an appeal of unconstitutionality against Organic Law 7/2021, considering the arguments and issues expressed in this document.

It is recommended that the European Ombudsman act with a view to preventing the use of facial recognition systems in Spain that violates the Fundamental Rights of articles 7, 8, 20 and 21 of the Charter of Fundamental Rights of the European Union.

RAPPORT SUR LES ASPECTS BIOETHIQUES, JURIDIQUES ET PROCEDURAUX DU DROIT A L'IDENTITE ET L'UTILISATION DES PROCEDURES DE RECONNAISSANCE FACIALE PAR LES FORCES ET LES ORGANES DE SECURITE

Paulo Ramon Suarez Xavier
Chercheuse postdoctorale Margarita Salas
Université de Malaga – Université de Barcelone
Observatoire de bioéthique et de droit

ÉTAT DU PROBLÈME

1. Perspective des procédures d'identification par les caractéristiques biologiques

Depuis l'avancée des technologies liées à l'identification des personnes par profils génétiques, c'est-à-dire au moyen de tests ADN, la manière d'identifier les personnes devant les autorités étatiques dans le cadre d'une procédure administrative et/ou judiciaire a été profondément modifiée.

Déjà à ce moment initial de l'avancement de la biotechnologie et des nanotechnologies, du moins en ce qui concerne l'affectation claire des droits fondamentaux

des citoyens, l'Observatoire de bioéthique et de droit de l'Université de Barcelone a adopté une position concernant la nécessité de sauvegarder les droits liés à la vie privée et familiale.

Si, à l'époque, le panorama présenté et l'essentiel des droits fondamentaux touchés par les procédures d'identification sur la base de profils ADN se limitaient à des questions moins complexes, telles que la protection des enfants et la validité des tests effectués en dehors d'une procédure judiciaire en l'altération de la paternité, l'avancée des nouvelles technologies et le big data ont mis en évidence la nécessité d'approfondir divers aspects, notamment la réutilisation à des fins d'exploitation des données de santé des usagers du système de santé public, une question également abordée par la loi et la bioéthique Observatoire dans un document de 2015.

Cependant, si nous nous concentrons sur ces questions différentes mais qui se recoupent, nous nous rendrons compte que l'un des éléments centraux des discussions qui se révèlent avec l'utilisation des données de santé et génétiques renvoie à l'identification des personnes et à laquelle nous avons convenu d'appeler " identité".

L'identité peut être définie de différentes manières, toutes correctes, comme un ensemble de caractères qui rendent un certain individu unique dans la communauté. On peut donc parler, plus qu'identité, d'identités, compte tenu du large spectre des possibilités d'individualisation d'une personne.

En ce sens, les progrès de la technologie ont permis l'adoption de nouvelles procédures d'identification des personnes par le biais de modèles, tels que la reconnaissance des empreintes digitales, la reconnaissance de l'iris et, plus récemment, la reconnaissance faciale.

Ces procédures d'identification révèlent des problèmes complexes. La première d'entre elles renvoie à la constitution de bases de données contenant des données biologiques et biométriques de citoyens, tant dans la sphère publique que privée, témoignant de la disparité de protection entre celles-ci et l'ADN, dont la constitution de bases de données est restreinte à quelques hypothèses bien précises établies par la loi organique. Loi 10/2007, du 8 octobre, réglementant la base de données policière sur les identifiants obtenus à partir de l'ADN et la dix-septième disposition supplémentaire de la

loi organique 03/2018, du 5 décembre, sur la protection des données personnelles et la garantie des droits numériques.

Dans le cas de la constitution de bases de données contenant des informations de données biométriques, y compris des images faciales, des données d'iris, des empreintes digitales et d'autres profils biométriques, une série de problèmes méritent d'être soulignés, car ils renvoient au même besoin de protection des données fondamentales droits des citoyens, indiqués dans les différents rapports préparés par l'OBD au cours des deux décennies.

2. Droit à l'identité et à l'identification

S'il existe différents processus et procédures d'identification des personnes et qu'ils utilisent pour la plupart la constitution de bases de données biométriques, biologiques, sanitaires et génétiques, dans quelle mesure leur utilisation peut-elle affecter les droits fondamentaux des citoyens ? Quels droits peuvent être affectés par ces mesures ?

Pour répondre à cette question, qui est d'une importance vitale pour ce document, nous devons recourir à un droit implicite dans les traités internationaux, mais explicitement déclaré par la Constitution espagnole: le droit à l'identité, traduit par le constituant dans le droit à sa propre image., garantie par la Constitution espagnole dans son article 18, section 1.

L'identité, l'image qu'un sujet a devant un groupe social et devant lui-même est un élément essentiel pour le libre développement de la personnalité. L'image, le visage, élément essentiel de l'identité du sujet est le reflet indélébile de la personnalité que la nature et la condition humaine elle-même confèrent à un membre d'une famille, d'une société.

En ce sens, le constituant a accordé une protection spéciale à l'image, à l'intimité personnelle, à la liberté idéologique et religieuse et, en définitive, à la dignité de la personne et au libre épanouissement de la personnalité, qui sont, dit le constituant, le fondement d'ordre politique et de paix sociale.

L'image définit l'identité individuelle et en est une partie vitale. Socialement, c'est la façon dont les gens s'identifient les uns aux autres dans la société, la famille et les institutions

et, juridiquement, c'est la première façon d'identifier les citoyens devant les pouvoirs publics.

Le droit à l'identité et à sa propre image est très personnel et, par conséquent, les sujets sont autorisés à influencer, même de manière invasive, leur propre image, en la modifiant par différentes formes d'action, par des procédures chirurgicales et non chirurgicales, naturelles ou par l'utilisation de ressources capables de modifier, selon la volonté de son propriétaire, les caractéristiques de son image.

Ce droit ne peut et ne doit pas être limité par des questions liées au fonctionnement des procédures d'identification. C'est parce que l'identité ne se confond pas avec l'identification. Le premier est un droit fondamental, tandis que le second est une obligation de l'État qui peut être satisfaite sous différents angles et selon les principes d'égalité de traitement et de non-discrimination, d'opportunité, de proportionnalité, d'efficacité, d'efficience et de responsabilité.

L'égalité de traitement implique que les procédures d'identification ne doivent générer aucune inégalité de sexe, d'origine, d'orientation sociale, d'orientation sexuelle ou toute autre forme de discrimination.

L'opportunité implique que la procédure d'identification doit avoir une base légale. En d'autres termes, elle doit viser à remplir les finalités légales qui lui sont assignées, qui sont la prévention de la commission d'infractions et l'identification des suspects, ou l'identification des responsables d'infractions administratives lorsque, compte tenu des circonstances, un concours est considéré nécessaires par les forces et organes de sécurité.

La proportionnalité fait référence aux moyens, impliquant la nécessité d'utiliser la mesure d'identification moins contraignante pour le citoyen qui se soumet à ladite procédure, ce qui implique que l'utilisation de procédures d'identification automatisées ostensives n'aurait aucune protection dans notre système juridique et dans notre système humain. système de protection des droits.

L'efficacité et l'efficience se réfèrent aux ressources et aux actions. Une procédure est efficace lorsqu'elle sert correctement les finalités établies, ne causant aucun dommage ou causant le moins de dommages possible (proportionnalité), auquel s'ajoute le besoin d'efficacité, c'est-

à-dire de réaliser ladite finalité avec le moins de gaspillage possible de ressources.

Bien qu'ils soient importants, ces principes ne peuvent pas outrepasser la pleine efficacité des droits fondamentaux et cela est établi à l'article 4 de la loi organique 04/2015, section 1, en réaffirmant la nécessité de respecter les droits fondamentaux des citoyens dans les actions de maintien et de restauration de la sécurité des citoyens et les pouvoirs spéciaux de la police administrative de sécurité.

En d'autres termes, les actions liées à l'identification susceptibles de porter atteinte au droit à l'identité garanti par la Constitution espagnole et les traités internationaux auxquels l'Espagne est partie, ainsi que les traités internationaux qui garantissent le droit à la dignité humaine, contredisent la logique de protection des droits fondamentaux, dépouillant le sujet de sa propre identité, de sa propre image, dans la mesure où les limitations imposées dépassent ce qui est strictement nécessaire au maintien de l'ordre public.

Il est du devoir de l'État de respecter l'identité et en même temps d'identifier les citoyens pour l'exercice de leurs droits et pour le maintien de l'ordre et de la paix sociale, afin de protéger le droit à l'image de soi des citoyens, ainsi que le droit à la protection des données personnelles.

3. Protection des données personnelles et identification

Les procédures d'identification, notamment les procédés de reconnaissance faciale par les systèmes de capture d'images et de sons sur la voie publique, portent atteinte non seulement au droit à sa propre image et au droit à l'identité, mais également au droit à la protection des données personnelles.

La protection des données personnelles des citoyens a eu sa première reconnaissance internationale avec la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, faite à Strasbourg le 28 janvier 1981, qui reconnaît comme des exceptions à la prescription générale pour le traitement des données à caractère personnel sans les garanties

nécessaires, le régime de protection de la sécurité de l'État et de la sécurité publique.

Dans le même ordre d'idées, l'article 8 de la Charte des droits fondamentaux de l'Union européenne définit le droit à la protection des données à caractère personnel comme l'une des libertés fondamentales au sein de l'Union européenne, interprétation à laquelle s'ajoute l'article 8 de la Convention européenne sur les droits de l'homme, en limitant la possibilité pour les autorités publiques d'interférer dans l'exercice de ces droits, sauf dans la mesure strictement nécessaire pour garantir la sécurité nationale, la sécurité publique, le bien-être économique du pays, la défense de l'ordre et la prévention des infractions pénales, la protection de la santé ou de la morale, ou la protection des droits et libertés d'autrui.

La protection des données, en ce sens, constitue un outil de droit, en vue de garantir la vie privée et familiale et l'identité des individus contre les ingérences indues dans leur spectre individuel et familial, donc la rectification, l'annulation et la consultation comme aspects fondamentaux de son exercice.

En d'autres termes, les données personnelles d'un individu constituent, dans une perspective bioéthique défendue par l'Observatoire de bioéthique et de droit, une part essentielle de la condition de personne du sujet dans la société numérique, lui permettant de s'intégrer librement au réseau en tant que membre de la société, avec le contrôle qu'il sera fait de leurs informations personnelles un usage strictement autorisé.

Cette idée, qui ouvre l'espace à des concepts tels que l'identité numérique auto-souveraine, dans laquelle l'individu a un contrôle total et absolu sur l'utilisation de ses données personnelles, comme s'il s'agissait d'un guichet unique, dont l'objectif est de remplacer le système déjà obsolète modèle d'avis et de choix actuellement incorporé dans notre législation.

La question fondamentale renvoie au fait que la loi organique relative à la protection des données et le règlement européen sur la protection des données ont exclu de leur champ d'application les traitements de données à des fins de prévention, de recherche, de détection ou de poursuite d'infractions pénales, ou d'exécution de sanctions pénales. sanctions, y compris la protection contre les menaces à la sécurité publique et leur prévention.

A) Directive UE 680/2016, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention, de recherche, de détection ou de poursuite d'infractions pénales ou d'exécution de sanctions et à la libre circulation de ces données

Dans ces domaines, qui incluent la protection de la sécurité publique, les dispositions de la directive UE 680/2016 sont appliquées, relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention, d'enquête, la détection ou la poursuite d'infractions pénales ou l'exécution de sanctions pénales, et la libre circulation de ces données.

Dans son article 3, la directive définit les données biométriques comme les données à caractère personnel obtenues à partir d'un traitement technique spécifique, liées aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique qui permettent ou confirment l'identification unique de ladite personne, telles que des images faciales ou données d'empreintes digitales.

Les données biométriques constituent, comme établi à l'article 10 de la directive, le groupe de données de catégorie spéciale, autorisées exclusivement lorsque cela est strictement nécessaire, sous réserve de garanties adéquates pour les droits et libertés de la partie intéressée et uniquement lorsqu'elles sont autorisées par le droit de l'Union ou de l'État membre; est nécessaire pour protéger les intérêts vitaux de l'intéressé ou d'une autre personne physique, ou lorsque ledit traitement se réfère à des données que l'intéressé a rendues manifestement publiques.

Curieusement, bien qu'elle mentionne la vidéosurveillance au considérant 26, la directive n'autorise pas explicitement l'utilisation de techniques de reconnaissance faciale ou l'utilisation de caméras de vidéosurveillance qui traitent des données personnelles en direct au moyen d'équipements mobiles ou fixes.

La vidéosurveillance à laquelle la directive fait référence dans ses considérants n'est pas la vidéosurveillance au moyen d'équipements permettant la reconnaissance faciale, mais l'utilisation de caméras pour enregistrer les événements qui se déroulent sur la voie publique et dont la réglementation

en Espagne a été donnée par la loi organique 04 /1997, du 4 août, qui réglemente l'utilisation des caméras vidéo par les forces et organismes de sécurité dans les lieux publics.

D'autre part, en ce qui concerne sa nature, il convient de noter que la directive UE 680/2016 constitue une directive de minimums, ce qui implique que les États membres peuvent élargir l'éventail des garanties contenues dans son texte, mais pas les restreindre, ce qui conduit à la nécessité d'examiner le texte législatif qui résulte de sa transposition.

B) Loi organique 7/2021, du 26 mai, sur la protection des données personnelles traitées à des fins de prévention, de détection, de recherche et de poursuite des infractions pénales et d'exécution des sanctions pénales

La loi organique 7/20221, du 26 mai, transpose la directive UE 680/2016 dans notre système juridique, bien qu'elle marque des distances dans une série de questions liées aux questions liées au traitement des données biométriques, car elle va bien au-delà de la dispositions de la norme européenne.

En effet, contrairement à la directive qui n'autorise qu'exceptionnellement l'utilisation des données biométriques, la loi organique autorise le traitement des données biométriques pour identifier de manière unique une personne, catégorie dans laquelle la reconnaissance faciale est incluse, sans autre exigence, ce qui implique une grave restriction du régime exceptionnel défini par l'article 10 de la Directive UE 690/2016.

Pour rendre viable l'utilisation de ces technologies, l'article 15 de la loi organique 7/2021, du 26 mai, autorise la captation d'images et de sons par les forces et organismes de sécurité sur la voie publique, en vue de permettre le traitement de données biométriques, sans précisant le régime d'autorisation de ces dispositifs, tel que recommandé par la loi organique 04/1997.

Ladite autorisation générique, qui exclut également le traitement des données biométriques à des fins d'identification dans le cadre du droit à l'honneur, à l'intimité personnelle et familiale et à sa propre image, aux fins des dispositions de l'article 2.2 de la loi organique 1/1982, constitue une violation flagrante des dispositions de l'article 18, paragraphes 1 et 4 de la Constitution espagnole.

Cabe destacar que la utilización de datos biométricos de los ciudadanos debería ser excepcional y aplicarse estrictamente para atender a necesidades puntuales, cuando esté en juego un interés público superior, sin que ello implique una presunción automática de este interés en cualquier actuación de las fuerzas y cuerpos de sécurité.

Cette large autorisation implique, en outre, une violation flagrante des droits fondamentaux proclamés dans la Charte des droits fondamentaux de l'Union européenne qui, dans ses articles 7 et 8, qui définissent les droits à la protection de la vie privée et familiale et le droit à la protection des données et à leur contrôle par une autorité indépendante.

Cette autorité, dans le cas de la loi organique 7/2021 du 26 mai, ne correspond pas au concept d'autorité indépendante, car elle relève des cas de traitement par le ministère public au sein du ministère public lui-même et du Conseil général. du pouvoir judiciaire dans les cas d'actions de procédure et dans divers organes dans le cas des forces et organismes de sécurité, ce qui implique un régime diffus et peu de sécurité pour les propriétaires des données traitées.

Ce régime suscite des inquiétudes de la part de l'Observatoire de bioéthique et de droit, qui y voit une série de risques pour la dignité humaine, des problèmes bioéthiques liés à la manipulation de l'information, la violation du droit à la liberté et au libre développement de la personnalité des groupes vulnérables et des minorités, ainsi que son utilisation possible à des fins indésirables par des États tiers qui reçoivent ces informations.

De telles considérations et la transposition inadéquate de la directive UE 680/2016 par le législateur espagnol, en introduisant des changements importants dans le régime de traitement des données biométriques, en modifiant la dynamique d'harmonisation maximale adoptée par la directive, exigent une position active de la part des institutions et société civile, pour la défense des droits fondamentaux.

C) La position du Médiateur concernant la constitutionnalité de la loi organique 7/2021, du 26 mai

Comme indiqué dans le rapport annuel du Médiateur pour l'année 2021, le haut-commissaire des Cortes Generales a reçu une demande citoyenne de présenter un recours d'inconstitutionnalité contre les articles 5, 9, 15, 17 et 24 de

la loi organique 7/2021, dont l'examen se trouve dans ledit rapport.

Dans ce document, le Médiateur souligne que la réglementation établie par la directive UE 680/2016 est comparable à celle régie par la directive UE 681/2016, concernant le registre des noms de passagers, puisque les deux sont déterminés par le même objectif de prévenir, d'enquêter et de poursuivre les crimes.

Rappelons, citant la doctrine de la Cour constitutionnelle, que la protection de la vie privée et la protection des données personnelles ne sont pas absolues et peuvent être limitées par une raison constitutionnellement pertinente, susceptible d'autoriser la restriction de ces droits dans la mesure nécessaire à la réalisation de ces extrémités.

Il conclut, après un examen de la proportionnalité, de la légalité de l'objectif et du modèle de garanties établi (essentiellement un système d'indemnisation pécuniaire et d'amendes), sur la constitutionnalité du règlement établi par la loi organique 7/2021, décidant de ne pas déposer de plainte recours.inconstitutionnalité.

La position du Haut Commissaire des Tribunaux sur une question aussi sensible préoccupe vivement l'Observatoire de bioéthique et de droit et les signataires de ce document, considérant, parmi de nombreux autres aspects, que le traitement des données biométriques ne peut être assimilé à l'Enregistrement des noms de passagers, puisqu'il s'agit dans ce cas des données d'identification les plus élémentaires du sujet, sans que cela soit lié à une atteinte à la vie privée et à l'image.

Deuxièmement, notamment en ce qui concerne les dispositions du paragraphe 2 de l'article 13 de la loi organique 7/2021, il n'établit pas de régime de garantie, mais autorise au contraire de manière illimitée la possibilité de traiter les données biométriques par les autorités compétentes, ce qui implique une autorisation pour le traitement de ces données, même pour les personnes qui ne sont pas soupçonnées ou qui ont été condamnées pour un crime.

Troisièmement, s'il est vrai qu'il n'y a pas de droits absolus, la restriction de droits fondamentaux aussi importants que le droit à l'image, à la protection des données et à la vie privée et familiale dans un État de droit dépend d'un système de

garanties qui permettent aux citoyens d'entrevoir que ces limitations sont une exception justifiée et non la règle, un aspect clairement ignoré dans la réglementation établie par l'article 13, section 2 et par les articles 15, 16 et 17 de la loi organique 7/2021.

Enfin, en ce qui concerne le système de garanties, il est préoccupant de considérer que le système disciplinaire établi par l'article 19 de la loi organique 7/2021 et par les droits à réparation prévus aux articles 53 (traitement par des entités publiques) et 54 (traitement par entités privées), suffisent à protéger les droits fondamentaux des citoyens contre des technologies dont il est prouvé qu'elles sont sujettes à des erreurs et dont les effets sur la vie des citoyens peuvent être désastreux à tous les niveaux.

L'Observatoire de bioéthique et de droit et les autres signataires de ce document rappellent que la liberté est une valeur supérieure dans la Constitution espagnole. Ce n'est pas par hasard que la liberté est mentionnée avant la justice dans l'article 1, puisque la justice sans liberté est l'oppression et la liberté sans la justice est l'anarchie.

La liberté doit prévaloir dans notre système juridique, qui fait partie de l'espace européen de liberté, de sécurité et de justice, dans lequel la même observation mentionnée ci-dessus s'applique, nous invitons donc le Haut Commissaire des Cortes Generales à revoir sa position concernant la constitutionnalité de la dispositions susmentionnées de la loi organique 7/2021, dont le contenu viole clairement les droits fondamentaux établis à l'article 18, paragraphes 1 et 4, ainsi que la protection des données et le droit au libre développement de la personnalité.

Cette position fait écho aux récentes manifestations du Parlement européen approuvées par le biais de la Résolution du 06 octobre 2021, sur le renseignement

en droit pénal et son utilisation par les autorités policières et judiciaires en matière pénale (2020/2016(INI)), qui appelle à l'interdiction permanente de l'utilisation d'autres caractéristiques humaines dans les espaces accessibles au public, telles que la marche, les empreintes digitales, l'ADN, voix et autres signaux biométriques et comportementaux.

La liberté est toujours le point de départ des propositions du Groupe d'avis de l'Observatoire de bioéthique et de droit,

à partir duquel sont établies les limites et la possibilité de restreindre l'exercice des droits fondamentaux. La restriction ne peut et ne doit pas être la mesure de la liberté, mais son exception, fondée sur la loi et protégée par une décision de justice lorsque l'entité de la restriction l'exige, comme c'est le cas avec l'utilisation des technologies de l'information et de la reconnaissance faciale.

DÉCLARATION

EXPOSÉ DES MOTIFS

Tenant compte que:

- Les données biométriques sont des données particulièrement sensibles et leur utilisation et traitement inappropriés peuvent générer une série de violations des Droits Fondamentaux;
- L'absence d'un cadre établi concernant la réutilisation des données biométriques par les entreprises et par les administrations publiques, notamment des personnes décédées;
- Les systèmes de reconnaissance faciale sont biaisés et leur utilisation par l'État en matière pénale peut affecter diverses minorités sociales;
- Les systèmes prédictifs peuvent établir des corrélations entre des ensembles de données, mais ne peuvent pas établir de relations causales ou prédire de manière fiable le comportement humain,
- L'identification du citoyen en tant que devoir et droit ne doit pas porter atteinte à son droit fondamental à l'identité;
- Le fonctionnement des algorithmes de reconnaissance faciale peut nécessiter des limitations sur l'utilisation d'accessoires, de maquillage, de voiles et d'autres aspects de l'image et de l'identité des citoyens;

Tenant compte que:

- La transposition de la directive UE 680/2016 n'a pas prévu d'autorité indépendante de contrôle du traitement des données à caractère personnel en matière pénale, mais a plutôt confié ces pouvoirs aux autorités de police, au ministère public et au Conseil général du pouvoir judiciaire;
- Le traitement des données biométriques sur la voie publique par les systèmes fixes et mobiles, en temps réel ou en différé, viole la présomption d'innocence et

le droit à l'identité des citoyens non soupçonnés d'avoir commis des délits et restreint leur liberté;
- Le fonctionnement des algorithmes de reconnaissance faciale peut nécessiter des limitations sur l'utilisation d'accessoires, de maquillage, de voiles et d'autres aspects de l'image et de l'identité des citoyens, limitant leur droit au libre développement de la personnalité;
- La réalisation de procédures esthétiques peut facilement contourner le fonctionnement des technologies de reconnaissance faciale et empêcher leur fonctionnement;
- Les risques qu'une fausse coïncidence peut engendrer pour le citoyen confondu avec une personne soupçonnée ou condamnée pour un crime;
- Le manque de clarté concernant les exigences et la manière de mener à bien la procédure d'identification.
- Le chercheur de l'Observatoire de bioéthique et de droit est parvenu à l'avis suivant

CONCLUSION

I - L'utilisation des technologies de reconnaissance faciale, de reconnaissance de formes et d'autres techniques algorithmiques visant à identifier les personnes ne doit pas être utilisée ostensiblement sur la voie publique, car elle présente une série de risques pour la liberté, l'identité et la vie privée des citoyens.

Son utilisation doit être limitée aux cas de nécessité et doit faire l'objet d'une autorisation judiciaire. Dans le cas contraire, la valeur supérieure de la liberté et les droits fondamentaux qui y sont liés seraient violés de manière flagrante.

II - L'utilisation des technologies de reconnaissance faciale dans les procédures d'identification peut générer des atteintes graves au droit fondamental au libre développement de la personnalité et au droit fondamental à l'identité, donc les actions nécessaires pour garantir son bon fonctionnement, telles que l'obligation de porter un visage nu, l'interdiction de l'utilisation de masques hyperréalistes ou de certains types de maquillage, finirait par causer plus de dégâts que l'utilisation d'autres technologies capables de garantir la sécurité des citoyens.

Il est recommandé que son utilisation, au cas où elle serait effectuée, se fasse de manière à protéger l'exercice légitime des droits fondamentaux, tels que l'identité et le libre développement de la personnalité, sans aucune discrimination, notamment religieuse .

III - Le système de contrôle de l'utilisation des données à caractère personnel en matière pénale, y compris les données biométriques, doit être soumis au contrôle d'une autorité indépendante, tel qu'établi à l'article 8 alinéa 3 de la Charte des droits fondamentaux de l'Union européenne. Le concept d'autorité de contrôle défini par la directive UE 680/2016 et la transposition effectuée par la loi organique 7/2021 contredisent ce précepte.

Il est recommandé d'apporter des modifications à la loi organique 7/2021, pour l'inclusion d'une autorité indépendante au lieu des autorités de contrôle et du système d'autorégulation actuellement prévus.

IV - En ce qui concerne la constitution de bases de données contenant des images biométriques de tous les

citoyens, promue par le règlement UE 2019/1157 dans son article 3, section 5, et son article 10. Son utilisation et son traitement doivent respecter les normes de garantie, en évitant le transfert de ces données vers des pays tiers dans lesquels il n'existe pas de système de garanties légales de leur utilisation et de leur réutilisation.

Il est recommandé de limiter l'utilisation commerciale qui peut être faite de ces données, notamment en vue d'éviter leur réutilisation pour la création de machines et de logiciels dont l'interface comporte un visage humain sans l'autorisation du propriétaire de l'image.

V - S'agissant de l'usage sur la voie publique d'appareils fixes et mobiles d'enregistrement d'images et de sons, avec possibilité de traitement de données personnelles et biométriques en temps réel ou différé, il est recommandé d'interdire leur usage ostentatoire, en conditionnant l'usage justifié que est mentionnée dans la première conclusion de son autorisation au moyen d'une décision judiciaire motivée et dûment adressée à l'autorité de protection des données.

En ce sens, il est recommandé de revoir la structure de la procédure établie dans les articles 15, 16 et 17 de la loi organique 7/2021.

VI – La configuration actuelle du système de protection des données en matière pénale, établie par la loi organique 7/2021, viole une série de droits fondamentaux, pour lesquels il est recommandé aux autorités légitimes de déposer un recours en inconstitutionnalité, c'est-à-dire les députés (50), Sénateurs (50) à adopter ladite mesure, notamment en ce qui concerne l'autorisation illimitée d'utilisation de la reconnaissance faciale constante à l'article 13, section 2.

Il est recommandé au Médiateur de réexaminer l'interprétation déclinée dans la décision de ne pas déposer de recours en inconstitutionnalité contre la loi organique 7/2021, compte tenu des arguments et des questions exprimés dans ce document.

Il est recommandé au Médiateur européen d'agir en vue d'empêcher l'utilisation de systèmes de reconnaissance faciale en Espagne qui viole les droits fondamentaux des articles 7, 8, 20 et 21 de la Charte des droits fondamentaux de l'Union européenne.

BERICHT ÜBER BIOETHISCHE, RECHTLICHE UND VERFAHRENSASPEKTE DES RECHTS AUF IDENTITÄT UND DIE VERWENDUNG VON GESICHTSERKENNUNGSVERFAHREN DURCH SICHERHEITSKRÄFTE UND -ORGANE

Paulo Ramón Suárez Xavier
Postdoktorandin Margarita Salas
Universität Málaga – Universität Barcelona
Observatorium für Bioethik und Recht

STAND DER AUSGABE

1. Perspektive von Identifizierungsverfahren durch biologische Merkmale

Seit der Weiterentwicklung von Technologien zur Identifizierung von Personen durch genetische Profile, d. h. durch DNA-Tests, hat sich die Art und Weise der Identifizierung von Personen vor den staatlichen Behörden in einem Verwaltungs- und/oder Gerichtsverfahren grundlegend verändert.

Bereits in diesem Anfangsmoment des Fortschritts der Bio- und Nanotechnologien, zumindest was die eindeutige Beeinträchtigung der Grundrechte der Bürger betrifft, hat die Beobachtungsstelle für Bioethik und Recht der Universität Barcelona eine Position bezogen auf die Notwendigkeit, die

Rechte zu wahren im Zusammenhang mit der persönlichen und familiären Privatsphäre.

Allerdings beschränkte sich damals der dargestellte Überblick und Kern der durch Identifizierungsverfahren anhand von DNA-Profilen berührten Grundrechte auf weniger komplexe Themen wie den Schutz von Kindern und die Aussagekraft von Tests, die außerhalb eines gerichtlichen Verfahrens durchgeführt wurden die Änderung der Vaterschaft, der Fortschritt neuer Technologien und Big Data haben die Notwendigkeit hervorgehoben, sich mit verschiedenen Aspekten zu befassen, einschließlich der Wiederverwendung von Gesundheitsdaten von Nutzern des öffentlichen Gesundheitssystems zu Zwecken der Nutzung, ein Thema, das auch von Law and Bioethics behandelt wird Beobachtungsstelle in einem Dokument von 2015.

Wenn wir uns jedoch auf diese unterschiedlichen, aber sich überschneidenden Themen konzentrieren, werden wir erkennen, dass sich eines der zentralen Elemente der Diskussionen, die sich mit der Verwendung von Gesundheits- und genetischen Daten ergeben, auf die Identifizierung von Personen bezieht und zu der wir uns bereit erklärt haben, „ Identität".

Identität kann auf verschiedene Weise definiert werden, alle richtig, als eine Reihe von Charakteren, die ein bestimmtes Individuum in der Gemeinschaft einzigartig machen. Es ist also möglich, mehr als Identität, von Identitäten zu sprechen, wenn man das breite Spektrum der Individualisierungsmöglichkeiten einer Person berücksichtigt.

In diesem Sinne hat der technologische Fortschritt die Einführung neuer Verfahren zur Personenidentifikation durch Muster ermöglicht, wie z. B. Fingerabdruckerkennung, Iriserkennung und in jüngerer Zeit Gesichtserkennung.

Diese Identifizierungsverfahren offenbaren einige komplexe Probleme. Die erste davon bezieht sich auf die Einrichtung von Datenbanken mit biologischen und biometrischen Daten von Bürgern, sowohl im öffentlichen als auch im privaten Bereich, was die Ungleichheit des Schutzes zwischen diesen und der DNA belegt, deren Einrichtung von Datenbanken auf einige sehr spezifische Annahmen beschränkt ist, die von Organic aufgestellt wurden Gesetz 10/2007 vom 8. Oktober zur Regelung der polizeilichen Datenbank über aus DNA gewonnene Identifikatoren und die siebzehnte Zusatzbestimmung des Organgesetzes 03/2018

vom 5. Dezember, Schutz personenbezogener Daten und Gewährleistung digitaler Rechte.

Im Falle der Einrichtung von Datenbanken mit biometrischen Dateninformationen, einschließlich Gesichtsbildern, Irisdaten, Fingerabdrücken und anderen biometrischen Profilen, gibt es eine Reihe von Aspekten, die hervorgehoben werden sollten, da sie sich auf denselben Grundschutzbedarf beziehen Rechte der Bürger, die in den verschiedenen Berichten angegeben sind, die das OBD in den zwei Jahrzehnten erstellt hat.

2. Recht auf Identität und Identifikation

Wenn es unterschiedliche Prozesse und Verfahren zur Identifizierung von Personen gibt und diese größtenteils auf die Erstellung biometrischer, biologischer, gesundheitlicher und genetischer Datenbanken zurückgreifen, inwieweit kann ihre Verwendung die Grundrechte der Bürger berühren? Welche Rechte können von diesen Maßnahmen betroffen sein?

Um diese Frage zu beantworten, die für dieses Dokument von entscheidender Bedeutung ist, müssen wir auf ein Recht zurückgreifen, das in internationalen Verträgen implizit enthalten ist, aber von der spanischen Verfassung ausdrücklich erklärt wird: das Recht auf Identität, das von den Wählern in das Recht am eigenen Bild übersetzt wird., garantiert durch die spanische Verfassung in Artikel 18, Abschnitt 1.

Die Identität, das Bild, das ein Subjekt vor einer sozialen Gruppe und vor sich selbst hat, ist ein wesentliches Element für die freie Entfaltung der Persönlichkeit. Das Bild, das Gesicht, ein wesentliches Element der Identität des Subjekts, ist die unauslöschliche Widerspiegelung der Persönlichkeit, die die Natur und das Menschsein selbst einem Mitglied einer Familie, der Gesellschaft verleihen.

In diesem Sinne hat der Verfassungsgeber dem Bild, der persönlichen Intimität, der Weltanschauungs- und Religionsfreiheit und letztlich der Würde des Menschen und der freien Entfaltung der Persönlichkeit, die das Fundament des Verfassungsgebers sind, besonderen Schutz gewährt der politischen Ordnung und des sozialen Friedens.

Das Bild definiert die individuelle Identität und ist ein wesentlicher Bestandteil davon. In sozialer Hinsicht ist es die Art und Weise, wie sich Menschen in Gesellschaft, Familie und Institutionen miteinander identifizieren, und rechtlich ist es die primäre Art, Bürger vor Behörden zu identifizieren.

Das Recht auf Identität und auf das eigene Bild ist sehr persönlich, und daher ist es den Subjekten erlaubt, ihr eigenes Bild auch auf invasive Weise zu beeinflussen, indem sie es durch verschiedene Aktionsformen, durch chirurgische und nicht-chirurgische Verfahren, natürlich oder durch die Verwendung von Ressourcen, die in der Lage sind, die Eigenschaften seines Bildes nach dem Willen seines Besitzers zu verändern.

Dieses Recht kann und sollte nicht durch Fragen im Zusammenhang mit der Durchführung von Identifizierungsverfahren eingeschränkt werden. Denn Identität wird nicht mit Identifikation verwechselt. Das erste ist ein Grundrecht, während das zweite eine Verpflichtung des Staates ist, die aus verschiedenen Perspektiven und unter den Grundsätzen der Gleichbehandlung und Nichtdiskriminierung, Chancengleichheit, Verhältnismäßigkeit, Wirksamkeit, Effizienz und Verantwortlichkeit erfüllt werden kann.

Gleichbehandlung bedeutet, dass Identifizierungsverfahren keine Ungleichbehandlung in Bezug auf Geschlecht, Herkunft, soziale Orientierung, sexuelle Orientierung oder andere Formen der Diskriminierung hervorrufen dürfen.

Die Möglichkeit impliziert, dass das Identifizierungsverfahren eine gesetzliche Grundlage haben muss. Mit anderen Worten, sie muss auf die Erfüllung der für sie festgelegten gesetzlichen Zwecke ausgerichtet sein, nämlich die Verhinderung der Begehung von Straftaten und die Ermittlung von Verdächtigen oder die Ermittlung der Verantwortlichen für Ordnungswidrigkeiten, wenn nach den Umständen ein Zusammentreffen in Betracht gezogen wird durch die Sicherheitskräfte und -organe erforderlich.

Verhältnismäßigkeit bezieht sich auf die Mittel, die die Notwendigkeit beinhalten, die Identifizierungsmaßnahme zu verwenden, die für den Bürger, der sich diesem Verfahren unterwirft, weniger belastend ist, was impliziert, dass die Verwendung angeblicher automatisierter Identifizierungsverfahren in unserem Rechtssystem und in unserem Menschen keinen Schutz hätte Rechteschutzsystem.

Effektivität und Effizienz beziehen sich auf Ressourcen und Maßnahmen. Ein Verfahren ist wirksam, wenn es den gesetzten Zwecken richtig dient, keinen Schaden verursacht oder den geringstmöglichen Schaden verursacht (Verhältnismäßigkeit), zu dem das Erfordernis der Effizienz hinzukommt, d. h. den Zweck mit möglichst geringem Ressourcenverbrauch zu erfüllen.

Obwohl sie wichtig sind, können diese Grundsätze die volle Wirksamkeit der Grundrechte nicht überwinden, und dies wird in Artikel 4 des Organgesetzes 04/2015, Abschnitt 1, festgelegt, indem die Notwendigkeit bekräftigt wird, die Grundrechte der Bürger bei Maßnahmen zur Aufrechterhaltung und Wiederherstellung zu beachten der Bürgersicherheit und die besonderen Befugnisse der Verwaltungssicherheitspolizei.

Mit anderen Worten, die Maßnahmen im Zusammenhang mit der Identifizierung, die das durch die spanische Verfassung und die internationalen Verträge, denen Spanien beigetreten ist, garantierte Recht auf Identität untergraben, sowie die internationalen Verträge, die das Recht auf Menschenwürde garantieren, widersprechen der Logik von Schutz der Grundrechte, Beraubung des Subjekts seiner eigenen Identität, seines eigenen Images, soweit die auferlegten Beschränkungen über das hinausgehen, was für die Aufrechterhaltung der öffentlichen Ordnung unbedingt erforderlich ist.

Es ist Aufgabe des Staates, die Identität der Bürgerinnen und Bürger zu achten und zugleich zur Wahrnehmung ihrer Rechte und zur Wahrung der Ordnung und des sozialen Friedens zu kennzeichnen, um das Recht auf Selbstdarstellung der Bürgerinnen und Bürger zu schützen, sowie das Recht auf Schutz personenbezogener Daten.

3. Schutz personenbezogener Daten und Identifizierung

Identifizierungsverfahren, insbesondere Gesichtserkennungsverfahren durch Bild- und Tonerfassungssysteme auf öffentlichen Straßen, untergraben nicht nur das Recht am eigenen Bild und das Recht auf Identität, sondern auch das Recht auf Schutz personenbezogener Daten.

Der Schutz personenbezogener Daten von Bürgern fand seine erste internationale Anerkennung mit dem am 28. Januar 1981 in Straßburg geschlossenen Übereinkommen zum Schutz von Personen bei der automatisierten Verarbeitung personenbezogener Daten, das eine der Ausnahmen von der allgemeinen Beschränkung anerkennt für die Verarbeitung personenbezogener Daten ohne angemessene Garantien des Regimes zum Schutz der Staatssicherheit und der öffentlichen Sicherheit.

In ähnlicher Weise definiert Artikel 8 der Charta der Grundrechte der Europäischen Union das Recht auf Schutz personenbezogener Daten als eine der Grundfreiheiten innerhalb der Europäischen Union, ein Verständnis, das durch Artikel 8 der Europäischen Konvention ergänzt wird zu den Menschenrechten, indem die Möglichkeit der Behörden eingeschränkt wird, in die Ausübung dieser Rechte einzugreifen, es sei denn, dies ist unbedingt erforderlich, um die nationale Sicherheit, die öffentliche Sicherheit, das wirtschaftliche Wohlergehen des Landes, die Verteidigung der Ordnung und die Verhütung von Straftaten zu gewährleisten, dem Schutz der Gesundheit oder der Sittlichkeit oder dem Schutz der Rechte und Freiheiten anderer.

Der Datenschutz stellt in diesem Sinne ein Rechtsinstrument dar, um die persönliche und familiäre Privatsphäre und die Identität von Personen vor unzulässigen Eingriffen in ihr individuelles und familiäres Spektrum zu schützen, daher sind Berichtigung, Löschung und Konsultation grundlegende Aspekte für seine Ausübung.

Mit anderen Worten, die personenbezogenen Daten einer Person stellen aus bioethischer Sicht, die von der Beobachtungsstelle für Bioethik und Recht verteidigt wird, einen wesentlichen Teil der Person des Subjekts in der digitalen Gesellschaft dar, die es ihm ermöglicht, sich als Mitglied frei in das Netzwerk zu integrieren der Gesellschaft, mit gebührender Kontrolle, dass ihre persönlichen Daten streng autorisiert verwendet werden.

Diese Idee, die Konzepten wie der selbstsouveränen digitalen Identität Raum gibt, bei der der Einzelne die vollständige und absolute Kontrolle über die Verwendung seiner persönlichen Daten hat, als wäre es ein einziges Fenster, dessen Ziel es ist, das bereits Veraltete zu ersetzen

Bekanntmachungs- und Wahlmodell, das derzeit in unserer Gesetzgebung enthalten ist.

Die grundlegende Frage bezieht sich auf die Tatsache, dass das Datenschutzgesetz und die Europäische Datenschutzverordnung die Verarbeitung von Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafverfolgung von ihrem Anwendungsbereich ausgenommen haben Sanktionen, einschließlich des Schutzes vor Bedrohungen der öffentlichen Sicherheit und ihrer Abwehr.

A) EU-Richtlinie 680/2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung und des freien Verkehrs solche Daten

In diesen Bereichen, zu denen auch der Schutz der öffentlichen Sicherheit gehört, werden die Bestimmungen der EU-Richtlinie 680/2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zu Präventions-, Ermittlungs-, die Aufdeckung oder Verfolgung von Straftaten oder die Vollstreckung strafrechtlicher Sanktionen und den freien Verkehr dieser Daten.

In ihrem Artikel 3 definiert die Richtlinie biometrische Daten als jene personenbezogenen Daten, die durch eine bestimmte technische Behandlung gewonnen werden und sich auf die physischen, physiologischen oder Verhaltensmerkmale einer natürlichen Person beziehen, die die eindeutige Identifizierung dieser Person ermöglichen oder bestätigen, wie z Fingerabdruckdaten.

Biometrische Daten stellen, wie in Artikel 10 der Richtlinie festgelegt, die Gruppe der Daten einer besonderen Kategorie dar, die ausschließlich zulässig sind, wenn dies unbedingt erforderlich ist, vorbehaltlich angemessener Garantien für die Rechte und Freiheiten der betroffenen Partei und nur dann, wenn dies zulässig ist des Mitgliedstaats; zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist oder wenn sich diese Behandlung auf Daten bezieht, die die betroffene Person offenkundig öffentlich gemacht hat.

Seltsamerweise erlaubt die Richtlinie, obwohl sie in Erwägungsgrund 26 die Videoüberwachung erwähnt, nicht ausdrücklich die Verwendung von Gesichtserkennungstechniken oder die Verwendung von Videoüberwachungskameras, die personenbezogene Daten live mit mobilen oder festen Geräten verarbeiten.

Die Videoüberwachung, auf die sich die Richtlinie in ihren Erwägungsgründen bezieht, ist keine Videoüberwachung mittels Ausrüstung, die eine Gesichtserkennung ermöglicht, sondern die Verwendung von Kameras zur Aufzeichnung von Ereignissen, die auf öffentlichen Straßen stattfinden und deren Regelung in Spanien durch das Organgesetz 04 gegeben wurde /1997 vom 4. August, das den Einsatz von Videokameras durch die Sicherheitskräfte und -organe an öffentlichen Orten regelt.

Andererseits ist im Hinblick auf ihren Charakter anzumerken, dass die EU-Richtlinie 680/2016 eine Mindestrichtlinie darstellt, was impliziert, dass die Mitgliedstaaten das Spektrum der in ihrem Text enthaltenen Garantien erweitern, aber nicht einschränken können, was führt uns zu der Notwendigkeit, den Gesetzestext zu prüfen, der sich aus seiner Umsetzung ergibt.

B) Organgesetz 7/2021 vom 26. Mai über den Schutz personenbezogener Daten, die zum Zwecke der Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten und der Vollstreckung strafrechtlicher Sanktionen verarbeitet werden

Das Organgesetz 7/20221 vom 26. Mai setzt die EU-Richtlinie 680/2016 in unser Rechtssystem um, obwohl es in einer Reihe von Fragen im Zusammenhang mit der Verarbeitung biometrischer Daten Distanzen markiert, da es weit über die hinausgeht Bestimmungen der europäischen Norm.

Im Gegensatz zur Richtlinie, die die Verwendung biometrischer Daten nur ausnahmsweise zulässt, erlaubt das Organgesetz ohne weiteres die Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer Person, eine Kategorie, in die die Gesichtserkennung eingeschlossen ist Einschränkung der Ausnahmeregelung gemäß Artikel 10 der EU-Richtlinie 690/2016.

Um die Nutzung dieser Technologien praktikabel zu machen, erlaubt Artikel 15 des Organgesetzes 7/2021 vom 26. Mai die Erfassung von Bild und Ton durch Sicherheitskräfte und -stellen auf öffentlichen Straßen, um die Datenverarbeitung zu ermöglichen biometrische Geräte, ohne Festlegung des Zulassungssystems für diese Geräte, wie im Organgesetz 04/1997 empfohlen.

Besagte allgemeine Genehmigung, die auch die Verarbeitung biometrischer Daten zum Zwecke der Identifizierung im Rahmen des Rechts auf Ehre, persönliche und familiäre Privatsphäre und das eigene Bild im Sinne der Bestimmungen von Artikel 2.2 des Organgesetzes 1/1982 ausschließt, stellt einen klaren Verstoß gegen die Bestimmungen von Artikel 18, Abschnitte 1 und 4 der spanischen Verfassung dar.

Es sei darauf hingewiesen, dass die Verwendung biometrischer Daten von Bürgern Ausnahmen sein und streng auf spezifische Bedürfnisse angewendet werden sollte, wenn ein höheres öffentliches Interesse auf dem Spiel steht, ohne dass dies eine automatische Vermutung dieses Interesses bei Maßnahmen der Streitkräfte und Organe impliziert Sicherheit.

Diese weitreichende Ermächtigung impliziert darüber hinaus einen klaren Verstoß gegen die in der Charta der Grundrechte der Europäischen Union proklamierten Grundrechte, die in ihren Artikeln 7 und 8 die Rechte auf Schutz des Privat- und Familienlebens und das Recht definieren zum Datenschutz und dessen Kontrolle durch eine unabhängige Stelle.

Diese Behörde entspricht im Fall des Organgesetzes 7/2021 vom 26. Mai nicht dem Konzept der unabhängigen Behörde, da sie Fälle betrifft, die von der Staatsanwaltschaft in der Staatsanwaltschaft selbst und im Generalrat behandelt werden der Justiz im Fall von Verfahrenshandlungen und in verschiedenen Gremien im Fall der Sicherheitskräfte und -organe, was ein diffuses Regime und wenig Sicherheit für die Eigentümer der verarbeiteten Daten impliziert.

Dieses Regime löst bei der Beobachtungsstelle für Bioethik und Recht Besorgnis aus, die eine Reihe von Risiken für die Menschenwürde, bioethische Probleme im Zusammenhang mit der Manipulation von Informationen, der Verletzung des Rechts auf Freiheit und der freien Entfaltung der Persönlichkeit

gefährdeter Gruppen sieht und Minderheiten sowie deren mögliche Verwendung für unerwünschte Zwecke durch Drittstaaten, die diese Informationen erhalten.

Solche Erwägungen und die unzureichende Umsetzung der EU-Richtlinie 680/2016 durch den spanischen Gesetzgeber durch die Einführung erheblicher Änderungen in der Verarbeitung biometrischer Daten, die Änderung der Dynamik der von der Richtlinie angenommenen maximalen Harmonisierung, erfordern eine aktive Haltung seitens der Institutionen und Zivilgesellschaft, zur Verteidigung der Grundrechte.

C) Die Position des Bürgerbeauftragten zur Verfassungsmäßigkeit des Organgesetzes 7/2021 vom 26. Mai

Wie im Jahresbericht des Bürgerbeauftragten für das Jahr 2021 angegeben, hat der Hochkommissar der Cortes Generales einen Bürgerantrag erhalten, eine Verfassungsbeschwerde gegen die Artikel 5, 9, 15, 17 und 24 des Organgesetzes 7/2021 einzureichen, deren Prüfung sich in besagtem Bericht findet.

Darin hebt der Ombudsmann hervor, dass die durch die EU-Richtlinie 680/2016 eingeführte Regelung mit der durch die EU-Richtlinie 681/2016 geregelten Regelung bezüglich des Fluggastregisters vergleichbar ist, da beide dem gleichen Zweck der Verhütung, Untersuchung und Verfolgung von Straftaten dienen.

Denken Sie unter Berufung auf die Lehre des Verfassungsgerichtshofs daran, dass der Schutz der Privatsphäre und der Schutz personenbezogener Daten nicht absolut ist und durch einen verfassungsrechtlich relevanten Grund eingeschränkt werden kann, der die Einschränkung dieser Rechte in dem für die Verwirklichung erforderlichen Umfang zulassen kann diese enden.

Sie kommt nach einer Prüfung der Verhältnismäßigkeit, Rechtmäßigkeit des Ziels und des festgelegten Garantiemodells (im Wesentlichen ein System der finanziellen Entschädigung und Geldstrafen) zur Verfassungsmäßigkeit der durch das Organgesetz 7/2021 eingeführten Verordnung und beschließt, keine Klage einzureichen Beschwerde. Verfassungswidrigkeit.

Die Position des Hohen Kommissars der Gerichte in Bezug auf ein so heikles Thema bereitet der Beobachtungsstelle für Bioethik und Recht und den Unterzeichnern dieses Dokuments große Besorgnis, da neben vielen anderen Aspekten die Verarbeitung biometrischer Daten nicht mit der Registrierung gleichgesetzt werden kann von Passagiernamen, da es sich in diesem Fall um die elementarsten Identifikationsdaten der betroffenen Person handelt, ohne dass dies mit einer Verletzung der Privatsphäre und des Ansehens verbunden ist.

Zweitens, insbesondere in Bezug auf die Bestimmungen von Artikel 13 Absatz 2 des Organgesetzes 7/2021, begründet es kein Garantieregime, sondern autorisiert stattdessen uneingeschränkt die Möglichkeit der Verarbeitung biometrischer Daten durch die zuständigen Behörden, was eine Genehmigung zur Verarbeitung dieser Daten auch für Personen, die nicht verdächtigt werden oder wegen einer Straftat verurteilt wurden.

Drittens gibt es zwar keine absoluten Rechte, aber die Einschränkung so wichtiger Grundrechte wie des Rechts am eigenen Bild, des Datenschutzes und der Privatsphäre der Person und Familie in einem Rechtsstaat hängt von einem System von Garantien ab, die dies gewährleisten die Bürger erkennen lassen, dass diese Beschränkungen eine begründete Ausnahme und nicht die Regel sind, ein Aspekt, der in der durch Artikel 13, Abschnitt 2 und durch Artikel 15, 16 und 17 des Organgesetzes 7/2021 festgelegten Verordnung eindeutig ignoriert wird.

Schließlich ist in Bezug auf das Garantiesystem zu bedenken, dass das durch Artikel 19 des Organgesetzes 7/2021 und durch die in den Artikeln 53 (Behandlung durch öffentliche Einrichtungen) und 54 (Behandlung durch private Einrichtungen) ausreichen, um die Grundrechte der Bürgerinnen und Bürger vor Technologien zu schützen, die nachweislich fehlerbehaftet sind und deren Auswirkungen auf das Leben der Bürgerinnen und Bürger auf allen Ebenen katastrophal sein können.

Das Observatorium für Bioethik und Recht und andere Unterzeichner dieses Dokuments erinnern daran, dass die Freiheit ein höherer Wert in der spanischen Verfassung ist. Nicht zufällig wird in Artikel 1 die Freiheit vor der Gerechtigkeit

erwähnt, denn Gerechtigkeit ohne Freiheit ist Unterdrückung und Freiheit ohne Gerechtigkeit Anarchie.

Freiheit muss in unserem Rechtssystem vorherrschen, das Teil des europäischen Raums der Freiheit, der Sicherheit und des Rechts ist, in dem die gleiche oben erwähnte Beobachtung zutrifft, weshalb wir den Hohen Kommissar der Cortes Generales einladen, seine Position in Bezug auf die Verfassungsmäßigkeit des Rechts zu überprüfen vorgenannten Bestimmungen des Organgesetzes 7/2021, deren Inhalt eindeutig gegen die in Art. 18 Abs. 1 und 4 verankerten Grundrechte sowie den Datenschutz und das Recht auf freie Entfaltung der Persönlichkeit verstößt.

Diese Position spiegelt die jüngsten Demonstrationen des Europäischen Parlaments wider, die mit der Entschließung vom 6. Oktober 2021 zu Geheimdiensten gebilligt wurden

im Strafrecht und seine Verwendung durch Polizei- und Justizbehörden in Strafsachen (2020/2016(INI)), die das dauerhafte Verbot der Verwendung anderer menschlicher Merkmale in öffentlich zugänglichen Räumen fordert, wie z. B. Gehen, Fingerabdrücke, DNA, Stimme und andere biometrische und Verhaltenssignale.

Freiheit ist immer der Ausgangspunkt der Vorschläge der Meinungsgruppe des Bioethik- und Rechtsobservatoriums, von dem aus die Grenzen und Möglichkeiten der Einschränkung der Ausübung von Grundrechten festgelegt werden. Die Einschränkung kann und sollte nicht das Maß der Freiheit sein, sondern ihre Ausnahme, die auf dem Gesetz basiert und durch ein Gerichtsurteil geschützt ist, wenn die Entität der Einschränkung dies erfordert, wie dies bei der Verwendung von Informationstechnologien der Fall ist.

AUSSAGE

BEGRÜNDUNG

In Anbetracht dessen:

- Biometrische Daten sind besonders sensible Daten, und ihre unangemessene Verwendung und Behandlung kann zu einer Reihe von Verletzungen der Grundrechte führen;
- Das Fehlen eines etablierten Rahmens für die Wiederverwendung biometrischer Daten durch Unternehmen und öffentliche Verwaltungen, insbesondere von verstorbenen Personen;
- Gesichtserkennungssysteme sind voreingenommen und ihre Verwendung durch den Staat in Strafsachen kann verschiedene soziale Minderheiten betreffen;
- Vorhersagesysteme können Korrelationen zwischen Datensätzen herstellen, aber keine kausalen Zusammenhänge herstellen oder menschliches Verhalten zuverlässig vorhersagen,
- Die Identifizierung des Bürgers als Pflicht und Recht sollte sein Grundrecht auf Identität nicht untergraben;
- Der Betrieb von Gesichtserkennungsalgorithmen kann Einschränkungen bei der Verwendung von Accessoires, Make-up, Schleier und anderen Aspekten des Images und der Identität der Bürger erfordern;

In Anbetracht dessen:

- Die Umsetzung der EU-Richtlinie 680/2016 hat keine unabhängige Behörde zur Kontrolle der Verarbeitung personenbezogener Daten in Strafsachen vorgesehen, sondern diese Befugnisse den Polizeibehörden, der Staatsanwaltschaft und dem Generalrat der Justiz übertragen;
- Die Verarbeitung biometrischer Daten auf öffentlichen Straßen durch feste und mobile Systeme, in Echtzeit oder zeitversetzt, verletzt die Unschuldsvermutung und das Recht auf Identität von Bürgern, die keiner Straftat

verdächtigt werden, und schränkt ihre Freiheit ein;
- Der Betrieb von Gesichtserkennungsalgorithmen kann Einschränkungen bei der Verwendung von Accessoires, Make-up, Schleier und anderen Aspekten des Images und der Identität von Bürgern erfordern, wodurch ihr Recht auf freie Entfaltung der Persönlichkeit eingeschränkt wird;
- Die Durchführung ästhetischer Verfahren kann den Betrieb von Gesichtserkennungstechnologien leicht umgehen und deren Betrieb verhindern;
- die Risiken, die ein falscher Zufall für den Bürger mit sich bringen kann, der mit einer Person verwechselt wird, die einer Straftat verdächtigt oder verurteilt wird;
- Die Unklarheit bezüglich der Anforderungen und der Art und Weise der Durchführung des Identifizierungsverfahrens.
- Der Wissenschaftler von Bioethics and Law Observatory hat Folgendes erreicht

SCHLUSSFOLGERUNGEN

I – Der Einsatz von Gesichtserkennungstechnologien, Mustererkennung und anderen algorithmischen Techniken zur Identifizierung von Personen sollte auf öffentlichen Straßen nicht auffällig eingesetzt werden, da er eine Reihe von Risiken für Freiheit, Identität und Privatsphäre der Bürger birgt.

Ihre Verwendung muss auf den Bedarfsfall beschränkt sein und es muss eine gerichtliche Genehmigung vorliegen. Andernfalls würden der höhere Wert der Freiheit und die damit verbundenen Grundrechte eklatant verletzt.

II – Der Einsatz von Gesichtserkennungstechnologien bei Identifizierungsverfahren kann zu schwerwiegenden Verletzungen des Grundrechts auf freie Entfaltung der Persönlichkeit und des Grundrechts auf Identität führen, daher sind die notwendigen Maßnahmen zur Gewährleistung seines ordnungsgemäßen Funktionierens erforderlich, wie z. B. die Verpflichtung zum Tragen eines Das bloße Gesicht, das Verbot der Verwendung hyperrealistischer Masken oder bestimmter Arten von Make-up würden am Ende mehr Schaden anrichten als der Einsatz anderer Technologien, die die Sicherheit der Bürger gewährleisten können.

Es wird empfohlen, dass seine Verwendung, falls sie durchgeführt wird, so erfolgt, dass die legitime Ausübung von Grundrechten wie Identität und die freie Entfaltung der Persönlichkeit ohne Diskriminierung, einschließlich religiöser Diskriminierung, geschützt wird .

III – Das Kontrollsystem für die Verwendung personenbezogener Daten in Strafsachen, einschließlich biometrischer Daten, muss der Kontrolle einer unabhängigen Behörde unterliegen, wie in Artikel 8 Absatz 3 der Grundrechte der Europäischen Union festgelegt. Dem widersprechen der Begriff der Kontrollbehörde durch die EU-Verordnung 680/2016 und die Umsetzung durch das Organgesetz 7/2021.

Es wird empfohlen, Änderungen am Organgesetz 7/2021 vorzunehmen, um eine unabhängige Behörde anstelle der derzeit geplanten Kontrollbehörden und des Selbstregulierungssystems aufzunehmen.

IV – In Bezug auf die Bildung von Datenbanken mit biometrischen Bildern aller Bürger, gefördert durch die EU-Verordnung 2019/1157 in Artikel 3, Abschnitt 5 und Artikel

10. Ihre Nutzung und Behandlung muss den Garantiestandards entsprechen und deren Übertragung vermeiden Daten in Drittländer, in denen es kein System gesetzlicher Garantien für ihre Verwendung und Weiterverwendung gibt.

Es wird empfohlen, die kommerzielle Nutzung dieser Daten einzuschränken, insbesondere um ihre Wiederverwendung für die Erstellung von Maschinen und Software zu vermeiden, deren Schnittstelle ein menschliches Gesicht ohne die Genehmigung des Eigentümers des Bildes enthält.

V – Im Hinblick auf die Verwendung von stationären und mobilen Bild- und Tonaufzeichnungsgeräten im öffentlichen Straßenverkehr mit der Möglichkeit, personenbezogene und biometrische Daten in Echtzeit oder zeitversetzt zu verarbeiten, wird empfohlen, deren auffällige Verwendung zu untersagen und die berechtigte Verwendung davon abhängig zu machen wird in der ersten Schlussfolgerung zu seiner Genehmigung durch eine begründete gerichtliche Entscheidung erwähnt und ordnungsgemäß an die Datenschutzbehörde weitergeleitet.

In diesem Sinne wird empfohlen, die Struktur des in den Artikeln 15, 16 und 17 des Organgesetzes 7/2021 festgelegten Verfahrens zu überprüfen.

VI – Die derzeitige Konfiguration des Datenschutzsystems in Strafsachen, die durch das Organgesetz 7/2021 festgelegt wurde, verletzt eine Reihe von Grundrechten, für die den legitimen Behörden empfohlen wird, eine Beschwerde wegen Verfassungswidrigkeit einzureichen, d), Senatoren (50), diese Maßnahme zu ergreifen, insbesondere in Bezug auf die uneingeschränkte Ermächtigung zur Nutzung der ständigen Gesichtserkennung in Artikel 13 Absatz 2.

Dem Ombudsmann wird empfohlen, die in der Entscheidung, keine Beschwerde wegen Verfassungswidrigkeit gegen das Organgesetz 7/2021 einzureichen, abgelehnte Einigung zu überprüfen und dabei die in diesem Dokument dargelegten Argumente und Probleme zu berücksichtigen.

Es wird empfohlen, dass der Europäische Bürgerbeauftragte tätig wird, um den Einsatz von Gesichtserkennungssystemen in Spanien zu verhindern, die gegen die Grundrechte der Artikel 7, 8, 20 und 21 der Charta der Grundrechte der Europäischen Union verstoßen.

INFORME SOBRE ASPECTOS BIOÉTICOS, LEGALES Y PROCESALES DEL DERECHO A LA IDENTIDAD Y EL USO DE PROCEDIMIENTOS DE RECONOCIMIENTO FACIAL POR LAS FUERZAS Y CUERPOS DE SEGURIDAD

Paulo Ramón Suárez Xavier
Investigador Posdoctoral Margarita Salas
Universidad de Málaga – Universidad de Barcelona
Observatorio de Bioética y Derecho

ESTADO DE LA CUESTIÓN

1. Perspectiva de los procedimientos de identificación por medio de características biológicas

Desde el avance de las tecnologías relativas a la identificación de personas por perfiles genéticos, es decir, por medio de pruebas de ADN, la forma de identificación de personas ante las autoridades estatales en un procedimiento administrativo y/o judicial se ha visto profundamente alterada.

Ya en aquel momento inicial del avance de la biotecnología y de las nanotecnologías, por lo menos en lo que se refiere a la clara afectación de los derechos fundamentales

de los ciudadanos, el Observatorio de Bioética y Derecho de la Universidad de Barcelona ha adoptado una postura respecto a la necesidad de salvaguardar los derechos relativos a la intimidad personal y familiar.

Si bien, en aquél momento, la panorámica que se presentaba y el núcleo de derechos fundamentales afectados por procedimientos de identificación basados en perfiles de ADN se restringía a cuestiones menos complejas, como la protección de la infancia y la validez de las pruebas realizadas fuera de un procedimiento judicial en la alteración de la paternidad, el avance de las nuevas tecnologías y del big data han puesto de relieve la necesidad de profundizar en diversos aspectos, incluyendo la reutilización con fines de explotación de los datos sanitarios de los usuarios del sistema de sanidad pública, tema también abordado por el Observatorio de Derecho y Bioética en documento del año 2015.

Sin embargo, si nos centramos en estas diferentes pero imbricadas cuestiones, nos percataremos que uno de los elementos centrales de las discusiones que son puestas de manifiesto con el uso de los datos sanitarios y genéticos se refiere a la identificación de las personas y al que hemos convenido denominar de «identidad».

La identidad puede ser definida de distintas formas, todas correctas, como un conjunto de caracteres que hacen de un determinado individuo único en la colectividad. Por lo que cabe hablar, más que de identidad, de identidades, teniendo en cuenta el amplio espectro de posibilidades de individualización de una persona.

En este sentido, el avance de las tecnologías ha permitido la adopción de nuevos procedimientos de identificación de persona por medio de patrones, como el reconocimiento por medio de huella digital, reconocimiento de iris y, más recientemente extendido, el reconocimiento facial.

Estos procedimientos de identificación ponen de manifiesto algunas cuestiones complejas. La primera de ellas se refiere a la constitución de bases que contengan datos biológicos y biométricos de los ciudadanos, tanto en el ámbito público cuanto en el privado, evidenciando la disparidad de protección entre estos y el ADN, cuya constitución de bases de datos se restringe a unos supuestos muy concretamente establecidos por la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores

obtenidos a partir del ADN y la disposición adicional decimoséptima de la Ley Orgánica 03/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

En el caso de la constitución de bases de datos con información de datos biométricos, incluyendo imágenes faciales, datos de iris, huellas y otros perfiles biométricos, hay una serie de cuestiones que merecen destaque, ya que se refieren a la misma necesidad de protección de los derechos fundamentales de los ciudadanos, señalada en los distintos informes elaborados por el OBD en las dos décadas.

2. Derecho a la identidad e identificación

Si existen distintos procesos y procedimientos para la identificación de las personas y, en su gran mayoría, emplean la constitución de bases de datos biométricos, biológicos, sanitarios y genéticos, ¿en qué medida su uso puede afectar a los derechos fundamentales de los ciudadanos? ¿qué derechos pueden ser afectados por estas medidas?

Para responder a esta pregunta, que tiene transcendencia vital para el presente documento, debemos recurrir a un derecho implícito en los tratados internacionales, pero explícitamente declarado por la Constitución Española: el derecho a la identidad, traducido por el constituyente en derecho a la propia imagen, garantizado por la Constitución Española en su artículo 18, apartado 1.

La identidad, la imagen que un sujeto ostenta frente a un grupo social y ante si mismo es un elemento esencial para el libre desarrollo de la personalidad. La imagen, el rostro, elemento esencial de la identidad del sujeto es el reflejo indeleble de la personalidad que la naturaleza y la propia condición humana otorga a un miembro de una familia, de la sociedad.

En este sentido, el constituyente ha dispensado una especial protección a la imagen, a la intimidad personal, a la libertad ideológica y religiosa y, en ultima instancia, a la dignidad de la persona y al libre desarrollo de la personalidad, que son, dice el constituyente, fundamento del orden político y de la paz social.

La imagen define la identidad individual y es parte vital de ella. Socialmente, es la forma por la cual las personas se

identifican entre si en la sociedad, familia e instituciones y, jurídicamente, es la forma primordial de identificación de los ciudadanos ante las autoridades públicas.

El derecho a identidad y a la propia imagen es personalísimo y, por ello, se permite a los sujetos incidir, inclusive de forma invasiva, en su propia imagen, cambiándola por medio de distintas formas de actuación, por medio de procedimientos quirúrgicos y no quirúrgicos, naturales o mediante la utilización de recursos capaces de alterar, de acuerdo con la voluntad de su titular, las características de su imagen.

Este derecho no puede ni debe ser limitado por cuestiones relativas al funcionamiento de procedimientos de identificación. Ello porque la identidad no se confunde con la identificación. La primera es un derecho fundamental, mientras que la segunda es una obligación del Estado que puede ser atendida desde distintas perspectivas y bajo los principios de igualdad de trato y no discriminación, oportunidad, proporcionalidad, eficacia, eficiencia y responsabilidad.

La igualdad de trato implica que los procedimientos de identificación no deben generar cualquier desigualdad con relación al sexo, origen, orientación social, orientación sexual o cualquier otra forma de discriminación.

La oportunidad implica que el procedimiento de identificación debe tener un fundamento legal. En otras palabras, debe estar direccionado al cumplimiento de los fines legales establecidos para ello, que son la prevención de la comisión de delitos y la identificación de los sospechosos, o bien para la identificación de responsables por infracciones administrativas cuando, en atención a las circunstancias concurrentes se considere necesario por parte de las fuerzas y cuerpos de seguridad.

La proporcionalidad se refiere a los medios, implicando en la necesidad de utilización de la medida de identificación que sea menos gravosa para el ciudadano que se somete a dicho procedimiento, lo que implica que la utilización de procedimientos de identificación automatizada de forma ostensiva no tendría amparo en nuestro ordenamiento jurídico y en nuestro sistema de protección de derechos humanos.

La eficacia y la eficiencia se refieren a los recursos y actuaciones. Un procedimiento es eficaz cuando sirve correctamente a los fines establecidos, no causando daños o cau-

sando el menor daño posible (proporcionalidad), a lo que se suma la necesidad de eficiencia, es decir, de realizar dicha finalidad con el menor dispendio de recursos posible.

Si bien son importantes, estos principios no pueden sobreponerse a la plena efectividad de los derechos fundamentales y así lo establece el artículo 4 de la Ley Orgánica 04/2015, apartado 1, al reafirmar la necesidad de observancia de los derechos fundamentales de los ciudadanos en las actuaciones para el mantenimiento y el restablecimiento de la seguridad ciudadana y las potestades especiales de la policía administrativa de seguridad.

Dicho de otra manera, las actuaciones relacionadas con la identificación capaces de menoscabar el derecho a la identidad que garantiza la Constitución Española y los tratados internacionales de los que España es parte, así como los tratados internacionales que garantizan el derecho a la dignidad humana, contradicen la lógica de protección de los derechos fundamentales, despojando al sujeto de la propia identidad, de su propia imagen, en la medida que las limitaciones impuestas excedan lo estrictamente necesario para el mantenimiento del orden público.

Es deber del Estado de respetar la identidad y a la vez identificar los ciudadanos para el ejercicio de sus derechos y para el mantenimiento del orden y de la paz social, de forma a proteger el derecho a propia imagen de los ciudadanos, así como el derecho a la protección de datos personales.

3. Protección de datos personales e identificación

Los procedimientos de identificación, especialmente los procesos de reconocimiento facial por medio de sistemas de captura de imagen y sonido en la vía pública enervan no apenas el derecho a propia imagen y el derecho a la identidad, sino también al derecho a la protección de datos personales.

La protección de los datos personales de los ciudadanos tuve su primer reconocimiento a nivel internacional con el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, que reconoce como una de las excepciones a la limitación general para

el tratamiento de datos personales sin las debidas garantías el régimen de protección de la seguridad del Estado y de la seguridad pública.

En la misma senda, el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea define el derecho a la protección de datos de carácter personal como una de las libertades fundamentales en el ámbito de la Unión Europea, comprensión a la que se suma el artículo 8 del Convenio Europeo de Derechos Humanos, al limitar la posibilidad de las autoridades públicas de realizar injerencias en el ejercicio de estos derechos, salvo en lo estrictamente necesario para garantizar la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

La protección de datos, en este sentido, constituye un derecho-herramienta, con vistas a garantizar la intimidad personal y familiar y la identidad de los individuos ante injerencias indebidas en su espectro individual y familiar, de ahí que se garantice la rectificación, la cancelación y la consulta como aspectos fundamentales para su ejercicio.

En otras palabras, los datos personales de un individuo constituyen, desde una perspectiva bioética defendida por el Observatorio de Bioética y Derecho, parte esencial de la condición de persona del sujeto en la sociedad digital, permitiendo que, libremente, se integre en la red como un miembro de la sociedad, con el debido control que de sus informaciones personales se hará el uso estrictamente autorizado.

Esta idea, que va abriendo espacio a conceptos como el de identidad digital auto-soberana, en la que el individuo tiene el total y absoluto control del uso de sus datos personales, como si se tratara de una ventanilla única, cuyo objetivo es sustituir el ya obsoleto modelo del notice and choice actualmente incorporado en nuestra legislación.

La cuestión fundamental se refiere al hecho de que la Ley Orgánica de Protección de datos y el Reglamento Europeo de Protección de Datos han excluido de su ámbito de aplicación el tratamiento de datos con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

A) La Directiva UE 680/2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos

En estos ámbitos, en los que se incluye la protección de la seguridad pública, se aplica lo dispuesto en la Directiva UE 680/2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos.

En su artículo 3, la Directiva define datos biométricos como aquellos datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o de conducta de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

Los datos biométricos constituyen, tal y como establece el artículo 10 de la Directiva, el grupo de los datos de categoría especial, permitida exclusivamente cuando sea estrictamente necesario, con sujeción a las salvaguardias adecuadas para los derechos y libertades del interesado y únicamente cuando lo autorice el Derecho de la Unión o del Estado miembro; sea necesario para proteger los intereses vitales del interesado o de otra persona física, o cuando dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos.

Curiosamente, aunque mencione la videovigilancia en su considerando 26, la Directiva no autoriza de forma explícita el uso de técnicas de reconocimiento facial ni tampoco el uso de cámaras de videovigilancia que realicen el tratamiento de datos personales en directo por medio de equipos móviles o fijos.

La videovigilancia a la que se refiere la Directiva en sus considerandos no es la videovigilancia por medio de equipos que permitan el reconocimiento facial, sino que el uso de cámaras para grabar los hechos que suceden en la vía pública y cuya regulación en España fue dada por la Ley Orgánica 04/1997, de 4 de agosto, por la que se regula la

utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

Por otro lado, en lo que se refiere a su naturaleza, cabe destacar que la Directiva UE 680/2016 constituye una Directiva de mínimos, lo que implica que los Estados miembros pueden ampliar el abanico de garantías constantes en su texto, pero no restringirlas, lo que nos conduce a la necesidad de examinar el texto legislativo que resulta de su transposición.

B) La Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales

La Ley Orgánica 7/20221, de 26 de mayo transpone la Directiva UE 680/2016 a nuestro ordenamiento jurídico, si bien marca distancias en una serie de cuestiones referentes a las cuestiones referentes al tratamiento de datos biométricos, ya que va mucho más allá de lo dispuesto en la norma europea.

En efecto, a diferencia de la Directiva, que autoriza apenas de forma excepcional el uso de datos biométricos, la Ley Orgánica autoriza el tratamiento de datos biométricos para identificar una persona de manera unívoca, categoría en la que se incluye el reconocimiento facial, sin más requisitos, lo que implica en una grave restricción del régimen excepcional definido por el artículo 10 de la Directiva UE 690/2016.

Para viabilizar la utilización de dichas tecnologías, el artículo 15 de la Ley Orgánica 7/2021, de 26 de mayo autoriza la captación de imagen y sonido por las fuerzas y cuerpos de seguridad en la vía pública, con vistas a permitir el tratamiento de datos biométricos, sin concretar el régimen de autorización de estos aparatos, tal y como preconizaba la Ley Orgánica 04/1997.

Dicha autorización genérica, que además excluye el tratamiento de los datos biométricos con fines de identificación del ámbito del derecho al honor, a la intimidad personal y familiar y a la propia imagen, a los efectos de lo establecido en el artículo 2.2 de la Ley Orgánica 1/1982, constituye una clara violación del dispuesto en el artículo 18, apartados 1 y 4 de la Constitución Española.

Cabe destacar que la utilización de datos biométricos de los ciudadanos debería ser excepcional y aplicarse estricta-

mente para atender a necesidades puntuales, cuando esté en juego un interés público superior, sin que ello implique una presunción automática de este interés en cualquier actuación de las fuerzas y cuerpos de seguridad.

Esta autorización tan amplia implica, otrosí, en una clara violación de los Derechos Fundamentales proclamado en la Carta de Derechos Fundamentales de la Unión Europea, que en sus artículos 7 y 8, que definen los derechos a la protección de la vida privada y familiar y el derecho a la protección de datos y a su control por una autoridad independiente.

Dicha autoridad, en el caso de la Ley Orgánica 7/2021, de 26 de mayo, no se corresponde con el concepto de autoridad independiente, ya que recae en los casos de tratamiento por el Ministerio Fiscal en el propio Ministerio Fiscal y en el Consejo General del Poder Judicial en los casos de actuaciones procesales y en diversos órganos en el caso de las Fuerzas y Cuerpos de Seguridad, lo que implica en un régimen difuso y de poca seguridad para los titulares de los datos tratados.

Dicho régimen genera preocupación por parte del Observatorio de Bioética y Derecho, que vislumbra una serie de riesgos para la dignidad humana, problemas bioéticos relacionados con la manipulación de la información, la violación del derecho a la libertar y al libre desarrollo de la personalidad de grupos vulnerables y minorías, así como su posible utilización para fines indeseables por parte de terceros estados que reciban esta información.

Tales consideraciones y la inadecuada transposición de la Directiva UE 680/2016 por parte del Legislador Español, al introducir sensibles cambios en el régimen de tratamiento de datos biométricos, alterando la dinámica de armonización máxima adoptada por la Directiva, reclaman una postura activa por parte de las instituciones y de la sociedad civil, en defensa de los derechos fundamentales.

C) La posición del Defensor del Pueblo en cuanto a la Constitucionalidad de la Ley Orgánica 7/2021, de 26 de mayo

Según consta en el informe anual del Defensor del Pueblo para el año 2021, el alto comisionado de las Cortes Generales ha recibido solicitud ciudadana para presentación de recurso de inconstitucionalidad frente a los artículos 5, 9, 15,

17 y 24 de la Ley Orgánica 7/2021, cuyo examen se encuentra en referido informe.

En él, el Defensor del Pueblo pone de relieve que la regulación establecida por la Directiva UE 680/2016 es equiparable al regulado por la Directiva UE 681/2016, referente al Registro de Nombres de Pasajeros, ya que ambas están determinadas por la misma finalidad, de prevenir, investigar y enjuiciar delitos.

Recuerda, citando la doctrina del Tribunal Constitucional, que la protección de la intimidad y la protección de datos personales no es absoluta y puede verse limitada por un motivo constitucionalmente relevante, capaz de autorizar la restricción de estos derechos en la medida que sea necesario para la consecución de estos fines.

Concluye, tras un examen de la proporcionalidad, licitud del objetivo y del modelo de garantías establecido (básicamente un régimen de reparación pecuniario y multas), sobre la constitucionalidad de la regulación establecida por la Ley Orgánica 7/2021, decidiendo por no interponer recurso de inconstitucionalidad.

El posicionamiento del alto comisionado de las Cortes Generales en cuanto a un tema tan sensible genera gran preocupación al Observatorio de Bioética y Derecho y a los firmantes del presente documento, considerando, entre muchos otros aspectos, que el tratamiento de datos biométricos no puede ser equiparado al Registro de Nombres de Pasajeros, ya que en este caso nos encontramos ante el dato más elementar de identificación del sujeto, sin que ello se relacione con una invasión en su privacidad y su imagen.

En segundo lugar, especialmente con relación a lo que dispone el apartado 2 del artículo 13 de la Ley Orgánica 7/2021, no establece un régimen de garantías, sino que se autoriza de forma irrestricta la posibilidad de tratamiento de datos biométricos por parte de las autoridades competentes, lo que implica en una autorización del tratamiento de estos datos inclusive para aquellas personas que no son sospechosas ni han sido condenadas por ningún delito.

En tercer lugar, si bien es verdad que no hay derechos absolutos, la restricción de derechos fundamentales de tan importante calado como el derecho a la propia imagen, a la protección de datos y a la intimidad personal y familiar en

un Estado de Derecho depende de un régimen de garantías que permitan a la ciudadanía vislumbrar que estas limitaciones son una justificada excepción, no la regla, aspecto claramente ignorado en la regulación establecida por el artículo 13, apartado 2 y por los artículos 15, 16 y 17 de la Ley Orgánica 7/2021.

Por último, en cuanto al régimen de garantías, genera preocupación considerar que el régimen disciplinario establecido por el artículo 19 de la Ley Orgánica 7/2021 y por los derechos a indemnización previstos por los artículos 53 (tratamiento por entes públicos) y 54 (tratamiento por entes privados), son suficientes para la protección de los derechos fundamentales de los ciudadanos frente a tecnologías que están comprobadamente sujetas a errores y cuyos efectos en la vida de los ciudadanos poden ser nefastos en todos los niveles.

El Observatorio de Bioética y Derecho y demás firmantes del presente documento recuerdan que la Libertad es un valor superior en la Constitución Española. No por casualidad se menciona la libertad antes de la justicia en el artículo 1, ya que la justicia sin libertad es opresión y la libertad sin justicia es anarquía.

La libertad debe primar en nuestro ordenamiento jurídico, que es parte del Espacio Europeo de libertad, seguridad y justicia, en el que se aplica la misma observación antes mencionada, por lo que invitamos al alto comisionado de las Cortes Generales a revisar su posición respecto a la constitucionalidad de los dispositivos antes comentados de la Ley Orgánica 7/2021, cuyo contenido viola claramente los derechos fundamentales establecidos en el artículo 18, apartados 1 y 4, así como a la protección de datos y el derecho al libre desarrollo de la personalidad.

Dicha postura hace eco de las recientes manifestaciones del Parlamento Europeo aprobada por medio de la Resolución de 06 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales (2020/2016(INI)), en la que se pide la prohibición permanente del uso de en espacios accesibles al público de otras características humanas, como los andares, las huellas dactilares, el ADN, la voz y otras señales biométricas y de comportamiento.

La libertad es siempre el punto de partida de las propuestas del Grupo de Opinión del Observatorio de Bioética y Derecho, a partir de la cual se establecen los límites y la posibilidad de restricción del ejercicio de derechos fundamentales. La restricción no puede ni debe ser la medida de la libertad, sino que su excepción, fundamentada en la ley y amparada por una sentencia judicial cuando la entidad de la restricción así lo exija, como lo es en el caso del uso de las tecnologías de reconocimiento facial.

DECLARACIÓN

EXPOSICIÓN DE MOTIVOS

Teniendo en cuenta que:

- Los datos biométricos son datos especialmente sensible y su uso y tratamiento inadecuado puede generar una serie de violaciones a Derechos Fundamentales;
- La ausencia de un marco establecido en cuanto a la reutilización de datos biométricos por empresas y por las administraciones públicas, especialmente de las personas fallecidas;
- Los sistemas de reconocimiento facial presentan sesgos y su uso por el Estado en el ámbito penal puede afectar a diversas minorías sociales;
- Los sistemas predictivos pueden hacer correlaciones entre conjunto de datos, pero no establecer relaciones de causalidad ni predecir con fiabilidad la conducta humana,
- La identificación del ciudadano como deber y derecho no debe menoscabar su derecho fundamental a la identidad;
- El funcionamiento de algoritmos de reconocimiento facial puede exigir limitaciones a la utilización de accesorios, maquillajes, velo, y otros aspectos de la imagen y de la identidad de los ciudadanos;

Teniendo en cuenta que:

- La transposición de la Directiva UE 680/2016 no ha previsto una autoridad independiente para el control de tratamiento de datos personales en materia penal, sino que han encomendado dichas competencias a las autoridades policiales, al Ministerio Fiscal y al Consejo General del Poder Judicial;
- El tratamiento de datos biométricos en la vía pública por sistemas fijos y muebles, en tiempo real o en diferido viola la presunción de inocencia y el derecho a la identidad de los ciudadanos que no son sospechosos de haber cometido delitos y restringe su libertad;
- El funcionamiento de algoritmos de reconocimiento fa-

cial puede exigir limitaciones a la utilización de accesorios, maquillajes, velo, y otros aspectos de la imagen y de la identidad de los ciudadanos, limitando su derecho al libre desarrollo de la personalidad;
- La realización de procedimientos estéticos puede fácilmente eludir el funcionamiento de tecnologías de reconocimiento facial e impedir su funcionamiento;
- Los riesgos que una coincidencia falsa pueda generar para el ciudadano que sea confundido con una persona sospechosa o condenada por un delito;
- La ausencia de claridad en cuanto a los requisitos y la forma de realización del procedimiento de identificación.
- El investigador del Observatorio de Bioética y Derecho, Dr. D. Paulo Ramón Suárez Xavier ha llegado a las siguientes

CONCLUSIONES

I – La utilización de tecnologías de reconocimiento facial, reconocimiento de patrones y demás técnicas algorítmicas destinadas a la identificación de personas no debe ser utilizada de forma ostensiva en la vía pública, ya que ofrece una serie de riesgos a la libertad, a la identidad y a privacidad de los ciudadanos.

Su uso debe restringirse a supuestos de necesidad y debe mediar autorización judicial para ello. De lo contrario, se estaría violando de forma flagrante el valor superior de la libertad y los derechos fundamentales conexos.

II – El uso de las tecnologías de reconocimiento facial en procedimientos de identificación puede generar graves violaciones al derecho fundamental al libre desarrollo de la personalidad y al derecho fundamental a la identidad, por lo que las actuaciones necesarias a garantizar su correcto funcionamiento, como la obligación de llevar el rostro desnudo, la prohibición de la utilización de máscaras hiperrealistas o de determinados tipos de maquillaje, terminarían produciendo más daños que la utilización de otras tecnologías capaces de garantizar la seguridad ciudadana.

Se recomienda que su uso, en el caso de que se realice, se haga de forma a proteger el legítimo ejercicio de los derechos fundamentales, como la identidad y el libre desarrollo de la personalidad, sin que medie cualquier discriminación, incluyendo la religiosa.

III – El régimen de control del uso que se hace de los datos personales en el ámbito penal, incluyendo los datos biométricos, debe estar sometido al control de una autoridad independiente, tal y como lo establece el artículo 8 apartado 3 de la Carta de Derechos Fundamentales de la Unión Europea. El concepto de autoridad de control definido por la Directiva UE 680/2016 y la transposición realizada por la Ley Orgánica 7/2021 contradicen dicho precepto.

Se recomienda la realización de cambios en la Ley Orgánica 7/2021, para la inclusión de una autoridad independiente en lugar de las autoridades de control y el sistema de autorregulación actualmente previstos.

IV – Con relación a la formación de bancos de datos conteniendo imágenes biométricas de todos los ciudadanos,

propiciados por el Reglamento UE 2019/1157 en su artículo 3, apartado 5, y artículo 10. Su utilización y tratamiento debe obedecer a unos estándares garantistas, evitándose la transferencia de estos datos a terceros países en los que no haya un sistema de garantías legales de su utilización y reutilización.

Se recomienda que se limite el uso comercial que se pueda hacer de estos datos, especialmente con vistas a evitar su reutilización para la creación de máquinas y softwares en cuya interface figure un rostro humano sin la autorización del titular de la imagen.

V – Con relación a la utilización de aparatos para toma de imagen y sonido fijos y móviles en la vía pública, con posibilidad de tratamiento de datos personales y biométricos en tiempo real o en diferido, se recomienda la prohibición de su utilización ostensiva, condicionando el uso justificado que se menciona en la conclusión primera a su autorización por medio de decisión judicial motivada y debidamente encaminada a la autoridad de protección de datos.

Se recomienda, en este sentido, la revisión de la estructuración del procedimiento establecido en los artículos 15, 16 y 17 de la Ley Orgánica 7/2021.

VI – La actual configuración del sistema de protección de datos en materia penal, establecido por la Ley Orgánica 7/2021 viola una serie de Derechos Fundamentales, por lo que se recomienda a las autoridades legitimadas para interponer recurso de inconstitucionalidad, es decir, Diputados (50), Senadores (50) a adoptar dicha medida, especialmente con relación a la autorización irrestricta para el uso de reconocimiento facial constante en el artículo 13, apartado 2.

Se recomienda al Defensor del Pueblo la revisión del entendimiento declinado en la decisión de no presentar recurso de inconstitucionalidad frente a la Ley Orgánica 7/2021, considerando los argumentos y cuestiones expresadas en el presente documento.

Se recomienda al Defensor del Pueblo Europeo, que actúe con vistas a impedir que se realice una utilización de sistemas de reconocimiento facial en España que viole a los Derechos Fundamentales de los artículos 7, 8, 20 y 21 de la Carta de Derechos Fundamentales de la Unión Europea.

EPÍLOGO

LA BIOÉTICA COMO RESPUESTA AL PANOPTISMO INTERINSTITUCIONAL Y LA VIGILANCIA PREDICTIVA

BIOETHICS AS A RESPONSE TO INTERINSTITUTIONAL PANOPTISM AND PREDICTIVE SURVEILLANCE

Paulo Ramón Suárez Xavier
Investigador Posdoctoral Margarita Salas
Universidad de Málaga – Universidad de Barcelona
Observatorio de Bioética y Derecho
ramonsuarez@uma.es/ramonsuarez@ub.edu

RESUMEN: El presente trabajo analiza los efectos que el uso de datos personales como forma de control social y recursos en materia de seguridad pública, especialmente los datos biométricos, puede ofrecer graves riesgos a la protección de los derechos fundamentales de los ciudadanos y reproducir la lógica del llamado panoptismo interinstitucional como forma de control social. Basa su análisis en la fundamental importancia de la bioética como zona de contacto con el derecho en contextos de la llamada sociología de emergencia.

Palabras clave: datos biométricos, panoptismo, panoptismo interinstitucional, bioética, nuevas tecnologías.

ABSTRACT: This paper analyzes the effects that the use of personal data as a form of social control and resources in matters of public security, especially biometric data, can offer serious risks to the protection of the fundamental rights of citizens and reproduce the logic of the so-called inter-institutional panopticism as a form of social control. He bases his analysis on the fundamental importance of bioethics as a zone of contact with law in contexts of what is conceptualized as emergency sociology.

Keywords: biometric data, panopticism, interinstitutional panopticism, bioethics, new technologies.

INTRODUCCIÓN

El uso de tecnologías disruptivas en distintos ámbitos de la vida y de la actividad humana está cambiando nuestra forma de ver y pensar la sociedad. En última estancia, está alterando la conformación de la propia arquitectura de la sociedad y de las ciudades, mediante la inclusión de nuevas tecnologías cuyo sentido fundamental, se sostiene, es garantizar mayor seguridad y derechos de los ciudadanos.

Dichas tecnologías, en su mayoría, emplean el tratamiento de determinados tipos de datos y operan mediante la interoperabilidad que, incluso de forma inadvertida, terminan por generar una gran cuantidad de datos personales que pueden y son tratados tanto por las empresas cuanto por el Estado, mediante un marco normativo plural, abarcando tanto la Ley Orgánica 3/2018, cuanto la Ley Orgánica 7/2021 y demás normas aplicables al tratamiento de estos datos.

Dicho fenómeno, de la algoritmización de la sociedad, opera en distintas velocidades y se instala en diferentes ámbitos, exigiendo del intérprete una visión no sectorial de las normas y derechos en materia de protección de datos y, a la vez, reclama una mirada crítica en cuanto a sus efectos sobre la sociedad en sí y, especialmente, en cuanto a los derechos fundamentales de las personas y a su propia condición humana.

Esta característica, relativa a la multifuncionalidad de la aplicación de la inteligencia artificial en distintos ámbitos de la

actividad humana, reclama la realización de análisis sectoriales que sean capaces de no perder de mira los efectos y consecuencias globales del uso de estos recursos tecnológicos.

En este sentido, el presente artículo busca analizar el uso de datos biométricos y faciales en materia de seguridad pública y control social, teniendo por base dos aspectos fundamentales. En primer lugar, analizando los efectos del uso masivo de estas tecnologías en materia de seguridad con relación a sus efectos en la propia concepción de control social y, en segundo lugar, respecto a la forma cómo la bioética encuentra su anclaje científico para responder a los riesgos ofrecidos por estas supuestas innovaciones.

Para ello, el trabajo comienza desgranando la concepción de vigilancia predictiva y la constitución del panóptico como un modelo de control social y arquitectónico que se está rediseñando en la actualidad y los efectos que ello supone para esta sociedad.

En segundo lugar, busca analizar los efectos que la denominada «Cuarta Revolución Industrial» o la llamada «Sociedad Red» impone en el rediseño de este modelo bajo el discurso del riesgo y cómo ello puede suponer una grave amenaza a los derechos fundamentales de los ciudadanos.

Por último, se analiza cómo la bioética puede configurar una respuesta contra-hegemónica a esta concepción emergente de seguridad y control social y su capacidad, desde el punto de vista epistemológico, de dar respuesta a las cuestiones y retos que se plantean.

2. VIGILANCIA PREDICTIVA Y CONTROL SOCIAL: BASES PARA LA CONSTRUCCIÓN DE UNA SOCIEDAD PANOPTICA

2.1. El panóptico como modelo de control social

El panóptico se ha ideado inicialmente como un modelo constructivo por (Benthan, 2000), se trata de una máquina óptica universal o, si se quiere, un dispositivo polivalente

aplicable a la vigilancia, mucho más allá de la prisión, se trata de un modelo capaz de abrigar habitantes involuntarios, reticentes o angostos.

Por su configuración, el panóptico permitiría al observador, el agente de la autoridad, la autoridad o quienes hagan su vez, controlar cada movimiento del custodiado, aislándole del mundo exterior, sin que este tenga la exacta consciencia sobre quien o desde donde se le vigila.

El modelo circular ideado por Bentham impone una brutal desigualdad entre el observado y el observador, ya que uno está encasillado, constreñido y bañado en la luz que invade su recinto de forma implacable, sin permitir un intercambio equivalente entre lo que es visto y lo que se deja ver a cambio.

Se trata de un modelo disciplinario, aplicable a instituciones penitenciarias, hospitales, escuelas, asilos, centros de trabajo y todo aquel espacio en el que se pueda establecer un sistema correccional, de control y en el que la libertad sea un elemento secundario y las instituciones sean un instrumento del sometimiento del individuo tutelado.

El panóptico invierte la lógica del calabozo y sus tres funciones (encerrar, privar de luz y ocultar) conservando solamente la primera de ellas (encerrar) liberando al agente disciplinario de la necesidad de adentrar la oscuridad para ejercer el control y la disciplina (Foucault, 2002).

La idea del panóptico es importante desde el punto de vista arquitectónico: se eliminan las celdas con grandes muros y los tumultos que concurren por veces al mismo tiempo en su interior, se impide el contacto entre los presos o entre los diferentes grupos de sujetos de la disciplina —recordemos que no solamente los presos son objeto de la lógica panóptica— por lo que, si son niños, no se pueden copiar entre ellos. En los hospitales, no hay ruidos, charlas o disipación de la atención (Foucault, 2002).

Ahora bien, la perspectiva panóptica no es solamente relacionada con el preso y a su concepción del mundo a su alrededor. Las instituciones panópticas también sufren cambios profundos en cuanto a su concepción organizacional. Pronto podremos identificar cómo muchas de estas concepciones están presentes en el modelo algorítmico que se implementan en nuestra sociedad.

En este sentido, como principal cambio institucional en el modelo disciplinario instaurado por la lógica del panoptismo, nos encontramos con la supresión del modelo masivo de agentes de la autoridad para controlar a todos y cada uno de los sujetos de la disciplina. En su lugar, se establece una vigilancia concentrada y puntual, oculta bajo la luz en lo que se ha concebido como una multiplicidad enumerada y controlada (Foucault, 2002).

Dicho de otra forma, la vigilancia del panóptico "confisca la mirada a su fruición, apropiándose del poder de ver y sometiendo al recluso" (Benthan, 2000), haciendo con que, en el edificio opaco y circular, no sean las sombras, pero sí la luz quien aprisione.

Esta invisibilidad alumbrada que caracteriza el panoptismo y el recelo del vigilado por no saber dónde, cómo ni de qué forma se le vigila, caracteriza una omnipotencia típica de los mecanismos de control psicológico o del fundamentalismo transcendental[1], que somete al sujeto no apenas física, como mentalmente, sea dentro o fuera de las instituciones de custodia.

2.2. Panoptismo y la imitación del dios

El panoptismo no surge del vacío. Sus raíces remontan a unos principios fundamentales que son la vigilancia y la invisibilidad. Cada uno de estos principios se justifican, en esta lógica, de forma independiente, bajo una lógica propia y con respecto a una organización específica.

La vigilancia se relaciona con la circularidad, implicando que todos los espacios del panóptico se pueden controlar de la mejor manera posible desde su punto neurálgico: su centro. El centro permite una economía de recursos humanos, porque excluye la multiplicidad de agentes necesarios al control, si no que también es donde reside el mayor ardil, al hurtar del observado el derecho de ser un observador y la consciencia del espacio, de la intermitencia de la mirada observadora y, más impone al observado una aparente omnipotencia por parte de la autoridad.

1 En este sentido, véase (Millet, 2000).

La omnipotencia somete el principio de vigilancia a una lógica invertida: menos vigilantes pueden controlar a más custodiados, haciendo nacer en estos un sentimiento de control permanente, que adviene de la constante invisibilidad y desnudez absoluta del custodiado, que pierde su individualidad al estar observado de forma permanente e ininterrumpida.

En este sentido, más que una máquina de control, el panóptico es un dios artificial, capaz de reciclar al marginal en una versión hodierna de esclavo: el proletariado (Castillo, 1998). Esta, pues, la diferencia básica entre el panoptismo puritano y la tortura inquisitorial y la que le hace más temido frente a él, de ahí que se diga a ese respecto que "el burgo es la antítesis de la fronda" (Castillo, 1998).

El debate, en este punto, es mucho más filosófico que práctico. No merece la pena, pues, discutir el cómo de Bentham y el qué de Foucault, pero es útil mencionar que el anclaje funcional de esta formulación se relaciona mucho más con el utilitarismo de Bentham y la idea de producir más y cumplir con un *munus* de la mejor y menos costosa forma, que la de permitir al sujeto custodiado una condición más digna.

Esta nos parece la condición fundamental que hace con que Foucault se decante por hacer una relectura filosófica de Bentham antes que resumirse a reproducir lo que ha dicho. Se trata de una cuestión importante, ya que Foucault concibe el panóptico como lo que es: una máquina de hacer el control social y sus interferencias sobre la condición impuesta al vigilado. En este sentido, hacer una relectura de la concepción del panóptico adoptada por Foucault para compararla con la idea defendida por Bentham sería un error[2].

Dicha lógica se asemeja invariablemente con la de una justificación transcendental del poder. En este sentido, lo que es imprescindible es que el poder, la fuerza de control sea visible, pero inverificable. Para el vigilado, la idea constante de estar siendo controlado, espiado, sin saber el momento exacto en el que se procesará la mirada puesta sobre sí (Foucault, 2002).

El poder del panóptico reside más en la distribución asimétrica e invisible del control que en una autoridad, ya que

2 Esta es la postura adoptada por algunos autores. Por todos, véase (Castillo, 1998).

recae en un individuo cualquiera que, en aquel momento, es vector que hace la lógica de vigilancia ser perpetuada por la propia lógica del panóptico.

Dicho de otra manera, el poder de la omnipotencia y omnipresencia del panóptico es invariablemente autopoiético y capaz de reproducirse por si mismo, lo que implementa la idea de divinidad de este mecanismo.

2.3. Panoptismo y control de los detalles

El panóptico no es exclusivamente una imitación de dios. En su incansable afán de controlarlo todo, el modelo se establece (especialmente en el Opúsculo de 1791) en lo que se denomina de doctrina de la minucia, que busca agotar todos los espacios con sus ventajas e inconvenientes, de ahí que se establezca una serie de doctrinas, como las del agua, del aire, de la tierra y del fuego, incluyendo intervenciones sobre la propia rutina del custodiado (como se vestirá, cuando descansará o se lavará), lo que permite una disociación entre el proyecto tal y como lo idealiza Bentham y su propia psicología individual.

Esta minucia en los detalles tiene una motivación profunda, y es que Bentham se centra en la doctrina de Helvecios sobre la educación y disciplina, que implica una relación profunda entre el hombre y el medio en el que se produce su personalidad (Helvétius, 1776), de ahí la importancia de expulsar la casualidad: el panóptico es el espacio del control absoluto.

Todo, absolutamente todo en el panóptico es pensado, evaluado, comparado y establecido. No hay nada en el panóptico que no tenga su razón de ser y todo lo que él establece tiene el propósito de mantener el custodiado sobre una situación de disciplina, de la cual el propio Bentham se ha visto víctima, ya que jamás tuvo tiempo para concluir su proyecto.

Todos estos detalles hacen del panóptico la materia visible de un control invisible. Tiene, sin embargo, una peculiaridad. El custodiado sabe que está bajo custodia. Aunque no comprenda cómo es visto, sí es capaz de comprender que se encuentra sobre un estado de disciplina y las limitaciones que ello implica para su condición personal.

Se trata de un elemento muy importante, sobre el que nos centraremos en los próximos epígrafes del presente trabajo. Sin embargo, quedémonos con la idea de que el panóptico impone un modelo de visibilidad absoluta para el custodiado.

2.4. Panoptismo y el utilitarismo del dolor

El panóptico tiene una base fundamental: en él, todo sirve a un fin determinado. También el descanso debe ser productivo en su visión. Esto es ser utilitarista. Bentham eleva la extensión de su utilitarismo hasta al máximo. Incluso el sufrimiento tiene una finalidad última: el control.

Por ello, el dolor no debe ser una medida adoptada sin cautelas. El sufrimiento debe estar relacionado a la huida del custodiado de las normas de la institución. Este el modelo que sienta la base disciplinaria que Foucault aleja de forma definitiva de su concepción de modelo disciplinar, ya que, por su sola presencia junto al condenado cantan a la justicia la alabanza de que aquella tiene necesidad: le garantizan que el cuerpo y el dolor no son los objetivos últimos de su acción punitiva (Foucault, 2002).

Sin embargo, de ello, el dolor, según Bentham, es también una herramienta de esta estructura. Sin ella no abrís disciplina. En este sentido podríamos afirmar que el dolor no es un objetivo, pero ocupa un espacio esencial de la teoría del panóptico de Bentham.

Llegando a este punto, cabría analizar qué relaciones este modelo tiene con nuestra sociedad.

3. LA SOCIEDAD RED Y EL PANÓPTICO INVISIBLE

3.1. La Sociedad Red y la (re)construcción del espacio por la legitimación

Para el geógrafo y político Milton Santos (Santos M., 2000) defiende que los distintos sistemas técnicos que provienen de diferentes épocas «*forman una situación y son una existencia*

en un lugar dado» que sirven para entender cómo se desarrolla el modo de vida, las conductas humanas en un determinado espacio. Pero es la forma de combinarlos el hecho determinante para identificar «cómo los residuos del pasado son un obstáculo para el futuro».

Dicha constatación es muy relevante, ya que indica: (i) que en las distintas sociedades en las que se distribuyen los diversos territorios de los estados modernos, la combinación de los recursos sociales, económicos y tecnológicos es determinante del modo de vida de cada una de ellas y (ii) que no solo los recursos, sino su aceptación e implantación más o menos extendida determinará las bases del *ethos*, del espacio circundante político, social y cultural de dicha sociedad.

Pero el fenómeno de la globalización y la irrupción de las nuevas tecnologías hizo surgir un nuevo escenario global, de rotura de fronteras[3] y apertura de los mercados, además del fenómeno ya examinado del e-Gobierno y la ciudadanía digital (Llano, 2016).

En este sentido, parte de la doctrina afirma que tal vez sea razonable entender el concepto de ciudadanía social como una forma de racionalización de la reducción de nuestras expectativas deliberativas. Buscamos en la tecnología una solución a la pérdida de legitimidad política de las sociedades occidentales. Hemos depositado en el contexto digital nuestras esperanzas de una domesticación de la globalización que no requiera de grandes cambios estructurales, de un progreso que apenas requiera un proceso de aprendizaje y adaptación cultural. Internet desproblematiza la generalización del tipo de vínculo social débil y electivo característico del comercio porque lo dota de un rostro amable. Las redes sociales son una especie de mercado sin dinero donde la organización emerge espontáneamente sin un entorno de normas comunes finalistas, sencillamente a través del juego de protocolos técnicos (Llano, 2016).

3 Un interesante análisis de dicho fenómeno desde una perspectiva europea es realizado por Jürgen Habermas. Para más sobre el tema véase Jürgen Habermas. (1998). La constelación posnacional. Barcelona: Ed. Paidós. Sobre dicho enfoque, Juan Carlos Velasco elabora una interesante teoría sobre gobernanza democrática en estos contextos de declive de poder de los Estados nacionales. Véase Velasco, J. «Constelación postnacional y gobernanza democrática». *Revista Dilemata. N.º 22,* año 8, pp. 163-182.

El desarrollo de esta sociedad basada en el fenómeno del *big data*, que avanza en distintas velocidades en los territorios y los mercados, trajo consigo los problemas de la pobreza y exclusión digitales, generando el fenómeno de la brecha digital.

Esta consiste en las diferencias de posibilidades de acceso a internet y servicios digitales por la población, en escenarios en los cuales una mayoría de la población mundial sigue sin tener acceso a dichos servicios (Santoyo, 2003). Pero la brecha digital no solamente afecta a las personas, sino que también se manifiesta entre los Estados, considerando la panorámica internacional, además de entre empresas y entre organizaciones públicas y privadas.

En el escenario actual, en el cual la vida social pasa a desarrollarse cada día más en contextos virtuales, el dominio de la información juega un papel crucial para todas las organizaciones.

Esta, quizás, sea la razón por la cual Kai-fu Lee señala la existencia de una batalla silenciosa por el control de la información y la carrera por el desarrollo de la inteligencia artificial (Lee, 2019).

Todos estos fenómenos, que como hemos señalado, ocurren en distintas velocidades entre los Estados y organizaciones, además de los distintos extractos sociales, originan lo que Manuel Castells denomina Sociedad en Red (Castells, 1997).

El autor, tras analizar la evolución histórica que tiene como marco la segunda guerra mundial, llega al concepto de la revolución tecnológica y pasa a identificar los paradigmas generados por la tecnología moderna. El primero de ellos es la información como base de trabajo de dichas tecnologías; el segundo sería la capacidad de penetración de los efectos de las nuevas tecnologías, moldeando la existencia humana por el medio tecnológico; el tercero sería la lógica de la interconexión de todo el sistema de tecnología, es decir, la interoperabilidad entre dichos recursos; el cuarto y con directa relación con el tercero es la flexibilidad, que significa la reversibilidad y posibilidad de modificación, adaptación de los recursos mediante la reordenación de sus componentes y por último, la convergencia creciente de tecnologías específicas en unos sistemas altamente integrados, dentro de los

cuales las mismas trayectorias tecnológicas individuales se integran, volviéndose prácticamente indistinguibles.

Dicha revolución ocurre primero, de forma silenciosa, con la expansión de los mercados de tecnología de la información y tiene como consecuencia fundamental la puesta a la disposición de una cantidad ilimitada de datos de la más diversa naturaleza, obligando la regulación del uso y procesamiento de dichas informaciones de naturaleza personal, culminando con los hodiernos reglamentos y normas protectoras de los datos personales en los distintos ordenamientos jurídicos.

También los entes públicos pasaron a recabar una enorme cantidad de información sobre las personas, sus aptitudes, calidades, vida cuotidiana, domicilio, situación económica y distintos otros aspectos por los cuales se desarrolla la vida social y política de las personas, motivo por el cual también para las organizaciones públicas se limita el tratamiento y acceso a dichos datos.

Dicho proceso, por otro lado, se manifiesta de forma distinta en la vida social en los días actuales. Es también Castells quien destaca que el desarrollo de esta identidad virtual y sus tensiones frente a la globalización y el proceso de deslegitimación de las instituciones por un proceso de cierre al diálogo y lucha por su propia supervivencia que destapa la crisis del Estado democrático, por su incapacidad para gestionar la contradictoria dinámica entre la Red y el Yo, entre la instrumentación de las vidas y el significado de la experiencia (Castells, Ruptura: la crisis de la democracia liberal, 2018).

La dinámica entre la Red y el Yo a la cual se refiere Castells es la misma tensión que, según Habermas, se establece entre facticidad y validez en la dicotomía «yo» y «nosotros», al referirse al sujeto como una invención liberal (Habermas, Direito e democracia: entre facticidade e validade, 1997).

Para el autor, el paso de la racionalidad moral dirigida a fines, que es la racionalidad colectiva y donde se centran los elementos centrales y críticos de la convivencia social, hacia la racionalidad moral práctica, establece una suerte de solipsismo social en el que el individuo pasa a ser su propio centro de atenciones y con ello, el concepto de bien común se diluye en el individualismo, lo que desencadena una crisis de legitimación institucional.

Solamente el consenso, en la visión de Habermas, podría dar lugar a soluciones plausibles para el problema, lo que demandaría una apertura por parte de los sectores sociales para llegar a un consenso real.

El mismo autor critica el activismo judicial en la toma de decisiones en el seno del proceso democrático, pero asume que las actuaciones judiciales para la concreción de los derechos sociales configuran la promoción de condiciones para la democracia, al sostener que si la limitación de la actividad judicial se deriva de la especial legitimación que caracteriza al procedimiento democrático, también debe tenerse en cuenta que el Poder Judicial, cuando hace efectivos determinados derechos sociales, actúa precisamente en el sentido de promover las condiciones de la democracia. En vez de apoderarse de prerrogativas que pertenecen a la deliberación mayoritaria, lo que hace el Poder Judicial cuando realiza derechos sociales fundamentales (Habermas, Direito e democracia: entre facticidade e validade, 1997).

El gran problema de la ética del discurso habermasiana como punto de partida para la legitimación es que, desde el punto de vista teórico, no admite un consenso ideal, por lo que la apertura, la verdad, veracidad y la intención de llegar a un consenso que son sus presupuestos básicos para el consenso terminarían por no concretarse en el mundo real. Es esta justamente la crítica de Karl-Otto Appel sobre la ética del discurso desde una perspectiva habermasiana (Apel, 2004).

Curiosamente, los defensores de la ética del discurso en los moldes de Karl-Otto Appel tampoco consiguen resolver el problema del fundamento último del consenso y apelan a la comunidad de investigadores de Charles Peirce para convertir el fundamento último del consenso en un fundamento metafísico, ya que, entonces, es la comunidad de investigadores y no el individuo el sujeto que conoce la verdad propiamente. Vemos que en el texto aparecen algunos rasgos característicos de esta comunidad a la que Peirce se refiere: esta no tiene límites y es capaz de aumentar su conocimiento. Esto tiene que ver con el hecho de que Peirce, cuando habla de comunidad de investigadores, no quiere significar comunidad de investigación actual, sino que el concepto abarca a todos los seres capaces de razonar, actuales, posibles y futuros (Bayas, 2008).

Dicho de otro modo, la Sociedad Red puede ser resumida en una sociedad de consumo, basada en el fenómeno del *big data*, la masificación del empleo de las redes sociales y con una fuerte tendencia hacia la desregulación, lo que hace surgir una crisis de legitimidad institucional y del propio Estado.

Algunos autores, como el procesalista José Joaquim Calmón de Passos (Passos, 1998) y el sociólogo Boaventura de Sousa Santos (Santos B. d., Pela mão de Alice: o social e o político na pós-modernidade, 2013) relacionan este proceso con las llamadas promesas de la modernidad, de libertad, igualdad y emancipación.

Para Boaventura la transición paradigmática ha sido entendida de dos maneras antagónicas. Por un lado, están quienes piensan que la transición paradigmática reside en una doble constatación: primero, que las promesas de la modernidad, luego de que dejó de reducir sus posibilidades a las del capitalismo, no fueron ni pueden ser cumplidas; y, en segundo lugar, que después de dos siglos de promiscuidad entre la modernidad y el capitalismo, tales promesas, muchas de ellas emancipadoras, no pueden cumplirse en términos modernos o en los términos diseñados por la modernidad. Lo verdaderamente característico del momento actual es que, por primera vez en este siglo, la crisis de regulación social va de la mano con la crisis de emancipación social. Esta versión de la transición paradigmática es lo que él denomina posmodernismo inquietante o de oposición (Santos B. d., Pela mão de Alice: o social e o político na pós-modernidade, 2013).

En cualquier caso, se trata de distintas formas de evaluar al mismo fenómeno. Y con ello queremos hacer referencia al liberalismo y al marxismo que, al inventar el individuo, también creó una promesa de emancipación y libertad que es contradictoria con el sistema burocrático e institucional que los Estados nación han diseñado en sus sistemas institucionales.

La propia noción de burocracia emergida desde una idea weberiana de organización de las Administraciones es incompatible con el sistema democrático, ya que la participación es restringida en dicho modelo.

Para remediar esta situación de demanda por participación popular, originada de los fenómenos a los cuales nos hemos referido antes, surgen los mecanismos de participación ciudadana y el intento de aproximación entre el Estado y la ciudadanía con el surgimiento de la gobernanza y meca-

nismos de participación a los cuales nos hemos referido en el capítulo anterior.

Sin embargo, aunque se vistiera con una nueva indumentaria, los fundamentos de la Administración han seguido siendo los mismos, dejando una vez más en manos de las promesas la tarea de apaciguar las inquietudes sociales.

En conclusión, la sociedad red y la digitalización del ejercicio de la ciudadanía, el fenómeno de las redes sociales y la implementación de la conectividad en diversos aspectos de la vida, lo que se llama algoritmización, no es solamente el reflejo de un cambio social, sino que también revela una nueva forma de control: un panoptismo interinstitucional, al que nos referiremos ahora.

3.2. La sociedad red y el panoptismo interinstitucional

Si en la sociedad red, la digitalización, el surgimiento de las redes sociales y la interoperabilidad entre sistemas, la interconexión entre el mundo físico y el virtual y la ruptura de la legitimación de las instituciones producen una quiebra de la confianza entre las personas y las instituciones, por otro lado, emerge una nueva forma de control social que no se encuentra contenida por un espacio ni tampoco destinada a un grupo concreto de personas: el panoptismo interinstitucional.

La noción de panoptismo institucional constituye - y este es el punto de partida de la comprensión que proponemos en este breve ensayo -un segundo paso, un perfeccionamiento de la lógica utilitarista de control imaginada por Bentham.

No se trata, es verdad, de un modelo de expoliación, sino más bien de un refinado modelo económico, social y político que se manifiesta desde distintas perspectivas y que tiene un impacto profundo en la condición humana y en la integración social, ya que termina por reducir la comprensión de las personas a una mera lógica numérico-estadística.

El modelo de panoptismo de la sociedad red difiere del ideado por Bentham en un aspecto fundamental. Y es que no se aplica de forma exclusiva en contextos disciplinarios y ni tampoco implica en la percepción del control por parte

del sujeto custodiado, especialmente considerando que esta lógica, la lógica del control, se justifica no por el eventual ilícito que realice el custodiado, sino que por los eventuales daños a los que se pueda exponer.

Dicho de otra forma, lo que legitima el modelo de panoptismo que se está implementando en la sociedad red se justifica por lo que la doctrina ha denominado como "sociedad del miedo" (Bude, 2017) o la "sociedad del control" (Alcántara, 2008), implicando un desplazamiento del discurso de la seguridad a todos los ámbitos de la vida humana.

La implementación de estos sistemas tiene como principal efecto lo que Alcántara denomina de tolerancia frente a la vigilancia. Con lo que se refiere a la capacidad de tolerar, de soportar medidas que limitan el libre albedrío y la intimidad sin que nazca una sensación de desasosiego y rechazo de las medidas de control, lo que va aumentando exponencialmente a lo largo del tiempo (Alcántara, 2008).

Dicho de otra forma, *el discurso sobre el que se construye este control en un mundo de redes está encaminado a enlazar directamente las medidas de control con la capacidad de gobierno de la sociedad actual. Los mensajes de la política del miedo y la guerra contra el terror persiguen crear un imaginario en el que un mundo distribuido no es gobernable en términos de promesas y de un futuro mejor, sino que la gobernabilidad misma pasa a estar definida en términos de seguridad, aunque en ningún momento se aclara si estas medidas protegen a los ciudadanos o a los poderes establecidos del ataque por parte de los propios ciudadanos* (Alcántara, 2008).

Este mismo discurso de la seguridad se ha ido asociando con otros discursos, como el nacionalismo y la idea de proteger la patria, la religión y la familia, con vistas a aislar y reprimir los críticos de estos modelos y permitir la asimilación de sus metodologías, así como la exclusión del otro.

Tales formas de control y de exclusión de minorías parece, por otro lado, configurar una reacción sistémica a las luchas por reconocimientos. Tales luchas, como bien destaca Habermas, tienen un parentesco que reside en un hecho fundamental: *son fenómenos que, aunque se encuentran emparentados, no deben ser confundidos. Su parentesco estriba en que tanto las mujeres, las minorías étnicas y culturales, así como las naciones y las culturas, ofrecen resistencia contra la opresión, la marginación y el desprecio, y de este modo*

luchan por el reconocimiento de las identidades colectivas, sea en el contexto de una cultura mayoritaria o en el de la comunidad de los pueblos. Se trata de movimientos de emancipación cuyos objetivos políticos colectivos se definen en primera instancia en clave cultural, aun cuando siempre estén en juego también desigualdades de carácter económico, así como dependencias de naturaleza política (Habermas, 1999).

Este modelo de control genera, desde nuestra visión, un descompás entre la autonomía privada de los ciudadanos que disfrutan de los mismos derechos y su autonomía ciudadana, produciendo lo que Habermas entiende como una interpretación «liberal» del sistema de los derechos que ignora la conexión entre ambas dimensiones (entre la autonomía privada y la autonomía ciudadana) y llega a malentender el universalismo de los derechos fundamentales como nivelación abstracta de las diferencias, es decir, como una nivelación tanto de las diferencias culturales como de las sociales (Habermas, 1999).

El Estado, en este sentido, así como grandes conglomerados empresariales, pasa a detener y controlar una gran cantidad de datos de los ciudadanos, elaborando perfiles, controlando sus movimientos por medio de cámaras en la vía pública y, ahora, apoderándose de sus rostros en bases de datos aparentemente inofensivas, pero que pueden tener efectos nefastos sobre la identidad y la condición humana.

Para comprenderlo, debemos abandonar brevemente el debate hermenéutico y fijarnos en los avances que la dogmática y la legislación positiva ha estado realizando en esta materia.

En primer lugar, la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, ha autorizado, con base en un determinado procedimiento y algunos matices, el uso de videocámaras en locales públicos, con vistas a garantizar la seguridad de los ciudadanos y, por otro lado, permitir que se cubra un mayor rango de espacio por el mismo agente de la autoridad.

En su exposición de motivos, el legislador sostiene que *la prevención de actos delictivos, la protección de las personas y la conservación y custodia de bienes que se encuentren en situación de peligro, y especialmente cuando las actuaciones perseguidas suceden en espacios abiertos al público,*

lleva a los miembros de las Fuerzas y Cuerpos de Seguridad al empleo de medios técnicos cada vez más sofisticados. Con estos medios, y en particular mediante el uso de sistemas de grabación de imágenes y sonidos y su posterior tratamiento, se incrementa sustancialmente el nivel de protección de los bienes y libertades de las personas.

Se nos fijamos, se trata de una inversión casi perniciosa. El control se justifica por la protección de los bienes y libertad de las personas, pero, efectivamente, ¿qué libertades se están tutelando por medio del control? Máxime cuando el propio artículo 2 de la ley, en su apartado 1 excluye el derecho al honor, a la intimidad personal y familiar y a la propia imagen, a los efectos de lo establecido en el artículo 2.2 de la Ley Orgánica 1/1982, del uso de estas tecnologías.

Ello implica en una conclusión invariable: en este sistema, el honor, la intimidad personal y familiar y la propia imagen ceden espacio para la seguridad, que asume un papel fundamental en las políticas del Estado.

Este escenario de ruptura de los derechos humanos frente a la seguridad se profundiza más con la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, que repite las disposiciones de su predecesora y excluye de su ámbito de aplicación los derechos fundamentales a la intimidad personal y familiar, a la propia imagen y al honor.

Su articulado permite el tratamiento de datos obtenidos por sistemas móviles y fijos en la vía pública, incluyendo los datos faciales que, poco a poco, se van integrando en las bases de datos del Estado (más allá de las ya constituidas por grandes empresas como Apple, Google y Facebook) por medio, en Europa, del Reglamento (UE) 2019/1157 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre el refuerzo de la seguridad de los documentos de identidad de los ciudadanos de la Unión y de los documentos de residencia expedidos a ciudadanos de la Unión y a los miembros de sus familias que ejerzan su derecho a la libre circulación, que en su artículo 3, apartado 5, impone la obligación de toma de una imagen facial del ciudadano identificado.

Así, la seguridad pasa a ser el valor fundamental de nuestra sociedad. En este sentido, Mitchell Gray, ya en el lejano 2003,

defendía que, en general, todos los argumentos en contra de las cámaras se aplica la vigilancia, porque las cámaras son el portador de la tecnología de reconocimiento facial. Lo que es más importante, los sistemas de vigilancia ponen en peligro la privacidad, y el desafío como crece la vigilancia es evitar que las soluciones de seguridad se conviertan en mayores amenazas para el tejido urbano que los que se supone que deben solucionar. La privacidad es inherentemente valiosa, cumpliendo una función crucial en el desarrollo de individuos y grupos (Grey, 2003).

El valor de la privacidad, para Michael Curry reside en el hecho de que este es el espacio de lo que hemos denominado de libre desarrollo de la personalidad. *Es en privado que las personas tienen la oportunidad de convertirse en individuos en el sentido en que pensamos del término. Las personas, después de todo, se convierten en individuos en el ámbito público, simplemente haciendo públicas selectivamente ciertas cosas sobre ellos mismos. Ya sea que se trate de ser selectivo con respecto a los puntos de vista religiosos o políticos, la historia laboral, la educación, los ingresos o la tez, el punto importante es este: en una sociedad compleja, las personas ajustan sus identidades públicas de la manera que creen mejor, y desarrollar esas identidades en entornos más privados* (Curry, 1997).

El desarrollo de estas tecnologías, en este sentido, termina por minar esta intimidad. Todo, absolutamente todo puede ser revisado, controlado y criticado, lo que hace añicos la idea de intimidad antes mencionada, absolutamente mermada por el modelo de protección de datos que, por un lado, impone una carga absurda de autogestión para el ciudadano y, por otro (como es el caso de la Ley Orgánica 7/2021), ignora totalmente los derechos a la intimidad personal y familiar y a la propia imagen, transformando toda la ciudad en el panóptico de Bentham, cuyas ventanas, los cristales que rompen la intimidad son los de las cámaras, no los de las ventanas.

De esta sociedad vigilada, sometida y cuya identidad, voluntariamente (e inocentemente) cedida, emergen sujetos de segunda categoría, prescindibles, herramientas de la sociedad y del Estado: un no miembro de la comunidad. Un hombre herramienta convertido en el *animal laborans* (Arendt, 2009).

Con el escenario de la tragedia a la vista, queda por cuestionar qué papel tiene el Derecho y cómo la bioética puede constituir una alternativa.

4. LA BIOÉTICA Y LOS DERECHOS HUMANOS COMO FORMAS DE REACCIÓN ANTI-HEGEMÓNICA

Los derechos no nacen ni se fundamentan por sí mismos. Les falta un sustrato moral, ético y social capaz de legitimar la imposición jurídica de un modelo adoptado por la mayoría a toda la sociedad, sin que ello, necesariamente, implique en la vulneración de los derechos que atañen aquellos ciudadanos que no hacen parte de esta mayoría.

Los fundamentos y reflexiones que nortean los principios inspiradores de estos cambios jurídicos, que se basan en el cambio social, encuentran su fundamento en una doble posibilidad: por un lado, el establecimiento de un plano de fondo sometido a máximas o, por otro, mediante la construcción discursiva y consensual de un marco absolutamente libre de dogmas y dirigido hacia la búsqueda del consenso.

Le llamamos a esta respuesta consensual ante retos consenso, porque la propia expresión verdad carga consigo la idea de dogma, de valor absoluto. No caben, en este sentido, la construcción de valores e ideas con validez absoluta cuando buscamos responder a los desafíos que se nos plantean en la actualidad como sociedad.

Por un lado, ya lo hemos dicho, nos encontramos con una tendencia fuerte al tratamiento de datos personales de los ciudadanos por las empresas y por el Estado, de forma que especialmente en el ámbito más invasivo para el libre desarrollo del individuo y la conformación de su identidad, se forma un entorno de permisividad al tratamiento de datos bajo escuetas y escasas limitaciones.

En este escenario, las tecnologías pasan a moldar no solamente el espacio a modo de panoptismo interinstitucional, más también la propia concepción del individuo que, sin haber querido ni consentido, pasa a formar parte de burbujas de control que tienden a violar la principal característica de

la naturaleza humana: su libertad viviente, el derecho a una identidad propia, la posesión de su propio rostro.

Lo curioso, en este caso, es que el cambio está siendo silencioso. A diferencia de los datos de ADN, que implicaban una operación al menos mínimamente invasiva y, en este sentido, más perceptible a los sujetos, la acción de toma (y no de cesión) de datos biométricos de los ciudadanos para la Administración es absolutamente insospechada, pero es indeleble y pasa a conformar la propia identidad actual y futura de la persona.

Este probablemente sea el fundamento precipuo de la inclusión de la bioética como respuesta y fundamento de estas cuestiones. Sus efectos sobre la propia condición humana, el derecho a decidir sobre su identidad, su rostro y los efectos que el uso de estas informaciones tiene para la intimidad, la identidad y la dignidad humana no tendría una respuesta interdisciplinar y contundente en otro ámbito científico.

Como destaca López Baroni (2015), la bioética en esta senda es el ágora en el que se comunican los especialistas de diferentes campos del conocimiento. Sus materias están acotadas en un extremo por la filosofía política y en el otro por la ciencia ficción. Su objeto es el estudio de cómo interacciona el hecho cultural humano, esto es, su naturaleza simbólica, con las leyes de la naturaleza. Aspira a crear reglas axiológicas universales antes de que sea demasiado tarde.

Esta concepción nos antepone la digitalización del cuerpo, las posibilidades, con la impresión 3D, de la reproducción de la identidad de un individuo físicamente o, con el *deep fake*, de forma virtual, lo que supone una suerte de comercio no del cuerpo en sí, pero de su conformación.

En este caso, el intercambio, a diferencia de los embates sobre el cuerpo humano como recurso, tal y como señala la mejor doctrina (Casado, 2016), es gratuito y ni siquiera podría ser considerado como intercambio. El Estado se adueña de la imagen facial del ciudadano.

Véase, a tenor de ejemplo, que la palabra Ley Orgánica 7/2021, de 26 de mayo no menciona siquiera la forma de obtención de estos datos (biométricos), ni menos la existencia de un deber de información de las autoridades a los ciudadanos sobre su uso.

Todo ello, como ya se ha puesto de manifiesto, tiene dos efectos fundamentales: el primer lugar, la conformación definitiva de lo que hemos denominado panoptismo interinstitucional y, en segundo lugar, la constitución de una amenaza permanente a la libertad, a los derechos fundamentales de los ciudadanos, especialmente el derecho a la identidad y a la intimidad personal y familiar.

Dicho de otro modo, el Estado no puede adueñarse de los datos faciales de todos los ciudadanos para tenerlos identificados en todo momento. Como pone de manifiesto Suárez Xavier (2021), refiriéndose a la Ley Orgánica 4/2015, la actividad delictiva preexistente o, al menos, la inminencia de su comisión, son los únicos supuestos que autorizan el simple procedimiento de exigencia de la identificación personal a los ciudadanos, incluyendo la exigencia de descubrimiento del rostro, cuando exista algún objeto que dificulte la identificación, por lo que la generalización de procedimiento, al margen de las circunstancias antes señaladas generan más inseguridad que las propias situaciones que con él se quiere cohibir.

Solamente una visión bioética del problema es capaz de traer a la luz los nefastos efectos del uso de estas tecnologías para la sociedad como un todo y para los derechos fundamentales de los ciudadanos, evitando el escenario descrito por Lecuona Ramírez (2020), para quien el uso de los datos personales no puede resultarnos indiferente. En la sociedad digital, todos somos relevantes. Es necesario crear ontologías24 para mejorar la toma de decisiones y estas necesitan numerosos conjuntos de datos. Nuestra información y nuestra identidad digital es objeto de deseo para la iniciativa pública y privada.

Imprescindible, pues, una respuesta bioética para el problema, que implica la adopción de dos perspectivas fundamentales: la primera, el respeto a la identidad y la autonomía de los ciudadanos sobre sus datos personales y, la segunda, el establecimiento de mecanismos de resistencia legal contra el fenómeno de panoptismo interinstitucional que se está instalando en el Espacio Europeo de Libertad, Seguridad y Justicia.

Dicha forma de resistencia, hemos dicho, encuentra su fundamento en las formas de reacción contra-hegemónica del Derecho.

La bioética, en este sentido, consistiría en lo que, en nuestra opinión, podría ser uno de los más importantes puntos o zonas de contacto (Santos B. d., 2005), definidas por el autor como *escenarios sociales donde mundos de vida normativa distinta entran en contacto y chocan. A menudo, las luchas cosmopolitas se desarrollan en tales escenarios sociales. Los mundos de vida normativa, además de ofrecer patrones de experiencias y expectativas económicas, políticas y sociales legítimas o autorizadas, recurren a postulados culturales muy amplios y, por tanto, los conflictos entre ellos suelen implicar asuntos, y movilizar fuerzas y energías que van más allá de lo que parece estar en juego en la versión manifiesta de los conflictos. Las zonas de contacto que me preocupan son aquellas en las que chocan culturas jurídicas diferentes de forma muy asimétrica, es decir, los choques que movilizan intercambios de poder muy desiguales*.

Según el autor, (Santos B. d., 2005) *lo que está en juego, en la zona de contacto, no es una simple determinación de igualdad o desigualdad, pues hay conceptos alternativos de igualdad presentes en la zona y en conflicto. En otras palabras, en la zona de contacto, la ley en pro de la igualdad no opera al margen de la ley en pro del reconocimiento de la diferencia. En la zona de contacto, la lucha legal cosmopolita es una lucha pluralista en pro de la igualdad de diferencias, transcultural o intercultural. Esta igualdad de diferencias incluye la igualdad de derecho transcultural de cada grupo presente en la zona de contacto a decidir si desea seguir siendo diferente o mezclarse con los otros y formar híbridos.*

Destaca que, *en la zona de contacto, las luchas cosmopolitas son especialmente complejas, y las constelaciones legales que de ella emergen suelen ser inestables, provisionales y reversibles. La lucha legal cosmopolita no es, en absoluto, el único tipo de lucha legal que se desarrolla en la zona de contacto* (Santos B. d., 2005).

Estas tensiones entre realidad, entre el ser y el deber ser, constituyen la principal forma de resistencia frente a cambios legales que no siempre parecen estar de acuerdo con la óptica de los derechos humanos y la bioética parece ser el único camino capaz de reafirmar la persona, su identidad y su libertad como centro del ordenamiento jurídico.

Las cuestiones están sobre la mesa. Resta seguir debatiendo.

CONCLUSIONES

Concluir una tarea de investigación si dar respuestas definitivas parece una tendencia en la actualidad, ya que casi todo está por ver, por decidir y por comprender.

En esta ocasión, no hay conclusiones provisionales. Todas, absolutamente todas las cuestiones sobre las que hemos discutido parecen tener una respuesta razonable y coherente desde el punto de vista de la bioética libre de dogmas, la bioética laica.

La persona, su dignidad, su identidad y el derecho que tiene de ser y existir en el mundo son el único dogma tolerable en esta óptica. Todos los demás aspectos del análisis, en este sentido, deben, necesariamente, estar supeditados a esta cuestión fundamental: el respeto hacía la dignidad y a los rasgos que definen la propia condición humana y que, por ello, se han llegado a denominar derechos humanos (la intimidad, la identidad, la libertad, son algunos de ellos).

La bioética, en este sentido, cuando discute el uso de datos biométricos y faciales y la construcción de esta lógica de control que hemos denominado panoptismo interinstitucional y que tiene por telón de fondo el discurso de la seguridad y del miedo, cumple una doble función: advierte de los riesgos que esta lógica impone a la existencia humana en su acepción más pura y pone de relieve la necesidad de limitar su uso, tal y como anteriormente se hizo con la constitución de las bases de datos de ADN.

En este papel, asume, en cuanto zona de contacto con el derecho, el papel fundamental de representar una reacción contrahegemónica frente a la tendencia de rotura de la lógica de la libertad por la lógica del control, del panoptismo antes señalado y los riesgos que ofrece.

En resumen, se trata de percibir que la implementación de un control tecnológico del comportamiento de los ciudadanos en la vía pública, por un lado, limita el libre desarrollo de la personalidad, estableciendo una lógica de control y observación sin límites, a modo de sociedad disciplinaria.

Por otro lado, rompe la idea de intimidad, definida como un «coto vedado», capaz de permitir al ciudadano reflexionar y decidir sobre sus posiciones. En síntesis, un respiro íntimo ante el control estatal que, mediante la implementación de

modelos de control basados en seguimiento tecnológico, reconocimiento facial en la vía pública y otras formas de control, termina por estar amenazado.

Resta pues, definir hasta qué punto puede y debe el Estado, en nombre de la seguridad y en defensa de amenazas etéreas e invisibles, en lo más de las veces, invadir este espacio de libre albedrío e intimidad, sin que ello implique el establecimiento de una sociedad disciplinaria, es decir, del modelo que llamados de panoptismo interinstitucional.

Se trata de un debate importante, cuyos reflejos y la postura que tomemos en cuanto sociedad marcará el mañana y que, muy probablemente, presentará reflejos inmediatos en nuestro presente. De ahí la importancia de la bioética: (re) pensar el hoy sin ignorar el mañana.

BIBLIOGRAFÍA

Alcántara, J. F. (2008). *La sociedad de control: privacidad, propiedad intelectual y el futuro de la libertad*. Barcelona: El Cobre Ed.

Apel, K.-O. (2004). *Com Habermas, contra Habermas: direito, discurso e democracia*. São Paulo: Landy.

Arendt, H. (2009). *La condición humana.* Barcelona: Ed. Paidós.

Baroni, M. L. (2015). *Bioética y Multiculturalismo: Políticas Públicas en España (1978-2013). El hecho cultural ante la revolución biotecnológica.* Barcelona: Universidad de Barcelona.

Bayas, M. (2008). Repositorio de la Universidad de Navarra. Fonte: unav.es/gep/IIIPeirceArgentinaBayas.html

Bayas, M. (s.d.). *La noción de comunidad en C. S. Peirce.* III Jornadas de Peirce en Argentina. Buenos Aires.

Benthan, J. (2000). *O Panóptico.* Belo Horizonte: Ed. Auténtica.

Bude, H. (2017). *La sociedad del miedo.* Barcelona: Ed. Herder.

Casado, M. (2016). «¿Gratuidad o precio? Sobre el cuerpo humano como recurso». Em M. C. (org), *De la solidaridad*

al mercado. El cuerpo humano y el comercio biotecnológico (pp. 17-34). Barcelona: Universidad de Barcelona.

Castells, M. (1997). *La sociedad red*. Madrid: Alianza Editorial.

Castells, M. (2018). *Ruptura: la crisis de la democracia liberal.* Madrid: Alianza Editorial.

Castillo, M. E. (diciembre de 1998). «El panóptico y la identificación de intereses». *Sobre algunas inexactitudes debidas a Michel Foucault y Elie Halévy.* Télog, pp. 57-93.

Curry, M. (1997). «The digital individual and the private realm». *Annals of the Association of American Geographers,* pp. 681-699.

Foucault, M. (2002). *Vigilar y castigar: nacimiento de la prisión.* Buenos Aires: Siglo XXI editores.

Grey, M. (2003). «Urban Surveillance and Panopticism: will we recognize the facial recognition society». *Surveillance & Society,* 1(3), pp. 314-330.

Habermas, J. (1997). *Direito e democracia: entre facticidade e validade.* Rio de Janeiro: Ed. Tempo Brasileiro.

Habermas, J. (1999). *La inclusión del otro: estudios de teoría política.* Barcelona: Paidós.

Helvétius, C. A. (1776). Helvétius, C. A. (1776). *De l'homme, de ses facultés intellectuelles & de son éducation.* Nakladatel není známý.

Lee, K.-F. (2019). *As superpotencias da inteligência artificial: China, Vale do Silicio e a nova ordem mundial.* Lisboa: Ed. Relógio D'Água.

Llano, C. M. (2016). «La ciudadanía digital ¿Ágora aumentada o individualismo post-materialista?» *Revista Latinoamericana de Tecnología Educativa,* 15 (2), pp. 15-24.

Millet, J. M. (n.º 75 de 2000). «Hegel y el fundamentalismo moderno». *Diálogos*, pp. 7-35.

Passos, J. J. (1998). *Democracia, Participação e processo.* São Paulo: Ed. Revista dos Tribunais.

Ramírez, I. D. (2020). «Aspectos éticos, legales y sociales del uso de la inteligencia artificial y el Big Data en salud en un contexto de pandemia». *Revista internacional de pensamiento político - I Época,* 15, pp. 139-166.

Santos, B. D. (2005). «El uso contra-hegemónico del derecho en la lucha por una globalización desde abajo». *Anales de la Cátedra Francisco Suárez, 39,* pp. 363-420.

Santos, B. D. (2013). *Pela mão de Alice: o social e o político na pós-modernidade.* Lisboa: Ed. Almedina.

Santos, M. (2000). *La naturaleza del espacio.* Barcelona: Ed. Ariel S.A.

Santoyo, A. S. (2003). *La brecha digital: mitos y realidades.* Baja California: Ed. Mexicali.

Xavier, P. R. (2021). *Reconocimiento facial y policía predictiva: entre seguridad y garantías procesales.* La Coruña: Colex.

CÓDIGOS **COMENTADOS**

COLEX

LA **EDITORIAL JURÍDICA** DE **REFERENCIA** PARA LOS **PROFESIONALES** DEL **DERECHO** DESDE **1981**

DESCUBRA MÁS OBRAS EN:

www.colex.es

Editorial Colex SL Tel.: 911 094 100 info@colex.es

La irrupción de las nuevas tecnologías ha cambiado la forma por la que los ciudadanos se relacionan entre sí, con el Estado y la dinámica de la vida misma. Cámaras de vigilancia, sensores de presencia, alarmas en los hogares y una gran gama de recursos tecnológicos han emergido para garantizar la seguridad dentro y fuera de los hogares.

En lo que respecta a la seguridad pública, también la vigilancia electrónica por medio de cámaras ha permitido multiplicar los ojos de las fuerzas y cuerpos de seguridad allá donde antes no podían llegar, por razones de plantilla, de tiempo y de procedimiento.

Estas cámaras, que antes potenciaban el ojo humano, ahora lo sustituye. Son capaces de identificar personas por medio de técnicas de reconocimiento facial y pueden ofrecer una serie de riesgos para los derechos y libertades de los ciudadanos.

En este sentido, en el presente informe se analizan los riesgos que su utilización presenta a nivel bioético, jurídico y procesal.

La presente obra se publica como resultado de las Ayudas a la Recualificación del Sistema Universitario Español 2022, en la Modalidad Ayudas Margarita Salas para la formación de jóvenes doctores, concedida a Paulo Ramón Suárez Xavier.

UNIVERSIDAD DE MÁLAGA
GOBIERNO DE ESPAÑA MINISTERIO DE UNIVERSIDADES
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

La presente investigación se realizó con apoyo de los siguientes centros de investigación:

Organización de las Naciones Unidas para la Educación, la Ciencia i la Cultura
uniTwin Cátedra UNESCO de Bioética de la Universitat de Barcelona
Observatori de Bioètica i Dret Universitat de Barcelona
KU LEUVEN CITIP CENTRE FOR IT & IP LAW

ISBN: 978-84-1359-855-0
9 788413 598550