Integración Regional & Derechos Humanos / Revista Regional Integration & Human Rights / Review

Año XI – Nº 2 – 2º semestre 2023

RI&HR Jean Monnet Centre of Excellence "Regional Integration and Human Rights"

Jean Monnet Centro de Excelencia "Integración Regional y Derechos Humanos" IR&DH

Cofinanciado por el programa Erasmus+ de la Unión Europea

Integración Regional & Derechos Humanos /Revista Regional Integration & Human Rights /Review

Revista del Centro de Excelencia Jean Monnet
Universidad de Buenos Aires – Argentina

Segunda época
Antigua *Revista Electrónica de la Cátedra Jean Monnet*
(2013 - 2019)

Año XI – N°2 – Segundo semestre 2023

ISSN: 2346-9196

Av. Figueroa Alcorta 2263 (C1425CKB)
Buenos Aires - Argentina
revistairydh@derecho.uba.ar

EL DERECHO AL RESPETO A LA VIDA PRIVADA: ¿EL PRECIO A PAGAR POR UNA EUROPA SEGURA EN LA ERA TECNOLÓGICA?

Andrea Garrido Raya[1]

Fecha de recepción: 4 de diciembre de 2023
Fecha de aceptación: 22 de diciembre de 2023

Resumen

A raíz del avance frenético de la revolución tecnológica los Estados disponen de una cantidad ingente de recursos "securitarios" tan eficaces y sofisticados como intrusivos y lesivos de derechos fundamentales. Entre ellos destacan los sistemas de reconocimiento facial y su aplicación para prevenir ilícitos y perseguir delitos a costa de la afectación, en particular, de los derechos vinculados a la privacidad, intimidad y protección de datos. Sobre esta temática versa la jurisprudencia más reciente del TEDH. Cuestiones de relevancia actual notable, como la implicación del proceso de la globalización digital en la teoría de los derechos fundamentales, el clásico debate seguridad/privacidad, o el conflicto Estado liberal (democrático) vs. Estado policial (autoritario), se están planteando ante los jueces de Estrasburgo. Pese a su enorme potencial, sus sentencias aportan más bien poco, pues aquellos tienden a dejar demasiadas preguntas en el aire.

Palabras clave: Reconocimiento facial - Derecho al respeto a la vida privada – Seguridad - Datos biométricos - Vigilancia masiva.

Title: THE RIGHT TO RESPECT FOR PRIVATE LIFE: THE PRICE TO BE PAID FOR A SECURE EUROPE IN THE TECHNOLOGICAL ERA?

Abstract

[1]Investigadora predoctoral FPU en el Departamento de Derecho Constitucional de la Universidad de Granada, España. Doctoranda en el Programa de Ciencias Jurídicas de la Universidad de Granada, España. Graduada en Derecho y Administración y Dirección de Empresas por la Universidad de Granada, España.

Technology is advancing at such an unstoppable rate that States are being provided with an enormous amount of security resources that are as effective and sophisticated as intrusive and harmful to fundamental rights. In this sense, the use of facial recognition technology in order to protect national security and prevent crime at the expense of rights related to privacy, intimacy and personal data is quite remarkable. The most recent ECtHR's jurisprudence concerns this matter. A great deal of relevant issues such as the implication of the process of digital globalisation in the theory of fundamental rights, or the classic security vs. privacy and liberal State vs. authoritarian State debates are currently being raised before the judges of Strasbourg. Their judgements, however, are to no avail due to the fact that the Court tends to leave too many questions unanswered.

Keywords: Facial recognition technology – Right to respect for private life – Security – Biometric data – Mass surveillance

I. La tríada seguridad, globalización tecnológica y derechos humanos

El derecho a la intimidad, o, en lenguaje convencional, el derecho al respeto a la vida privada (art. 8 CEDH), es un derecho en demolición (REVENGA SÁNCHEZ, 2016). Lo que antaño se erigía en la piedra angular del Estado liberal no es más que una reliquia del pasado.

Como resalta REVENGA SÁNCHEZ (*Ibidem*: p.82), es evidente que nuestro estilo de vida actual no se caracteriza por tomar demasiado en serio el valor de lo privado o lo íntimo. El ciudadano que en el s. XIX daba su vida por disfrutar de su intimidad e individualidad al margen de cualquier injerencia externa, pública o privada, hoy exhibe en Internet sus quehaceres cotidianos y sus datos personales siendo plenamente consciente (o no) de que con ello genera un rastro de trazabilidad susceptible de ser almacenado, utilizado y comercializado por una cantidad ingente de organismos públicos y privados. Los primeros, además, parece que han olvidado el fundamento de su poder, mostrándose proclives a devaluar la eficacia de los derechos de los ciudadanos al someter a aquellos, más frecuente que excepcionalmente, a la imperiosa necesidad de preservar la seguridad y el orden público nacional.

No en vano, los sistemas de vigilancia están presentes por doquier. La obsesión "securitaria" que emerge a principios del s. XXI ha conseguido pervertir los cimientos democráticos sobre los que se sustenta el Estado constitucional, hasta el punto de convertirse éste en una especie de Estado policía que evoca al panóptico de BENTHAM o al *Big Brother* de ORWELL en tanto que regímenes totalitarios y de vigilancia perpetua (*Ibidem:* pp. 83-84). Ello se ha visto acrecentado por los avances derivados del proceso de la globalización tecnológica, que han promovido la creación de nuevos y sofisticados sistemas de seguimiento y control cuya ejecución conlleva un riesgo de intrusión en los derechos intrínsecos a la privacidad del individuo (MARTÍN Y PÉREZ DE NANCLARES, 2008: p. 210).

Claro ejemplo de esto último es la creciente y generalizada implantación de cámaras de videovigilancia y reconocimiento facial en la vía pública, las cuales, al haber sido perfeccionadas mediante Inteligencia artificial, permiten tomar una cara y compararla con otras imágenes previamente almacenadas en diversas bases de datos[2], con el objetivo de encontrar una correspondencia que permita identificar a la primera de forma inequívoca[3]. Su instalación en las infraestructuras públicas más concurridas constituye uno de los principales medios de investigación y prevención de ilícitos en países como Estados Unidos, China (RIDAURA MARTÍNEZ, 2023: pp. 269 y 272) o Rusia. Así, por ejemplo, en 2017 se instalaron en Moscú más de tres mil quinientas cámaras de televisión de circuito cerrado (CCTV), de entre las cuales más de tres mil fueron equipadas con tecnología de reconocimiento facial en tiempo real[4]. En 2018, además, se

[2]Las bases de datos que utiliza el sistema como referencia o estándar de comparación pueden proceder de diversas fuentes; desde archivos policiales antiguos hasta imágenes o grabaciones publicadas en la red.

[3]Nos encontramos en el terreno de los datos biométricos, que se pueden definir como aquellos datos personales relacionados con las características fisiológicas, conductuales o físicas -imagen facial- de una persona, cuyo tratamiento y análisis posibilita su identificación y autentificación.

[4]La propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia artificial (Ley de Inteligencia artificial) y se modifican determinados actos legislativos de la Unión, distingue entre sistema de identificación biométrica remota "en tiempo real" (art. 3 (37)) y "en diferido" (art. 3 (38)). En el primero la recogida de los datos biométricos, la comparación y la identificación se producen sin una demora significativa, esto es, mínima o incluso instantánea. Mientras que el segundo se corresponde con todo aquel sistema de identificación biométrica remota que no encaje dentro de esa definición;

procedió a la instalación de varias cámaras de vigilancia en el metro de la capital. Esta política de rastreo indiscriminado de la ciudadanía alcanza su punto álgido en 2020; momento en el que ya todas las cámaras de la ciudad (aproximadamente ciento setenta y cinco mil en 2020 y doscientas veinte mil en 2022) se encuentran equipadas con tecnología de reconocimiento facial en tiempo real[5].

Esta alarmante cuestión nos reconduce a la tensión que rige las dialécticas entre las nociones de seguridad y privacidad/libertad, las cuales, al ser traídas al contexto actual, encuentran su máxima expresión en la colisión que se produce entre los Estados tecnológicos de la vigilancia y las voces de la conciencia democrática (REVENGA SÁNCHEZ, 2023: p. 249). No en vano, el empleo recurrente e indiscriminado de técnicas de reconocimiento facial no solo implica la restricción directa del derecho a la protección de la privacidad, de la propia imagen o de los datos personales, sino que también afecta, aunque sea de forma indirecta, a otros tantos derechos inherentes al individuo y al Estado social y democrático de Derecho; como el derecho a la libertad de expresión, a la de reunión o a la presunción de inocencia (RIDAURA MARTÍNEZ, 2023: p. 270).

II. La restricción legítima de derechos convencionales. Un breve repaso en torno a la doctrina sentada por el Tribunal de Estrasburgo

Esto último lo refleja la novedosa sentencia dictada por el Tribunal Europeo de Derechos Humanos (TEDH) en torno al asunto *Glukhin v. Russia.* Con ella la Corte europea tiene la posibilidad, por primera vez, de pronunciarse de forma directa sobre la compatibilidad (o no) del empleo de técnicas de reconocimiento facial con el Convenio Europeo de Derechos Humanos (CEDH). O, más concretamente, sobre si la aplicación de este tipo de tecnología sobre el demandante por parte de las autoridades rusas supuso una injerencia que desborda el "escudo de legitimidad" del que disponen los Estados a la hora de restringir derechos convencionales. Se trata, en definitiva, de dilucidar si Rusia

Bruselas, 21.4.2021 COM (2021) 206 final 2021/0106 (COD). Texto accesible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52021PC0206

[5]STEDH *Glukhin v. Russia,* 04/07/23, apartado 5.

supera o no el “test de Estrasburgo”, que consiste, tras verificar que el derecho convencional (art. 8.1 CEDH) ha sido efectivamente sometido a algún tipo de restricción, en comprobar si la misma encuentra justificación conforme a los requisitos y condiciones avaladas por la propia Convención (art. 8.2 CEDH). A saber, en este caso: que la injerencia venga previamente recogida y regulada con la suficiente precisión y calidad en la ley nacional, que responda a un objetivo legítimo (como el de garantizar la seguridad y el orden público) y que sea, además, necesaria en una sociedad democrática, es decir, que no vaya más allá de lo que exige o requiere esta última (REVENGA SÁNCHEZ, 2023: p. 251). Tales formalidades son, en buena medida, análogas a las dispuestas por los arts. 9.2, 10.2 y 11.2 CEDH. Así lo corrobora, de hecho, el fallo de la sentencia al condenar a Rusia por violación (también) del art. 10.1 CEDH[6].

La primera de las exigencias, relativa a la previsión legal de la restricción, consiste en comprobar si la intromisión encuentra fundamento en el derecho interno, incluyéndose aquí tanto el derecho no escrito como la jurisprudencia de los tribunales. Este requisito ha de ser entendido en sentido material y no solo formal, lo que significa que la Corte valora su concurrencia a la luz del estándar identificado como “calidad de la ley”. Es decir, para apreciar que la intromisión está efectivamente prevista en el régimen legal, es necesario que este último recoja la restricción junto con ciertas garantías que disipen las posibilidades de abuso por parte de los poderes públicos. Lo que sucede cuando la ley es accesible y está formulada con la suficiente precisión, pues con ello se garantiza que el ciudadano puede dirigir su conducta en función de las consecuencias predicables de la comisión de un acto ilegal. En ese sentido, el Tribunal suele ser especialmente exigente a la hora de enjuiciar la calidad de la ley que regula los sistemas de vigilancia masivos y/o secretos, o, como se verá a continuación, de obtención y procesamiento de datos sensibles[7] (PÉREZ DE LOS COBOS ORIHUEL, 2018: p. 38). Si la Corte no aprecia la previsibilidad legal de la intromisión pública, ésta sentencia su ilegitimidad y la violación del art. 8 CEDH sin entrar a valorar la concurrencia del resto de requisitos. De llegar a considerar,

[6]Apartados 54-57.
[7]Apartados 76-77.

por el contrario, que la restricción sí que encuentra fundamento en el derecho nacional, se procede entonces a determinar si la misma responde a un objetivo legítimo, *p.ej.,* protección de los derechos de terceros o defensa del orden público.

Finalmente, además de estar prevista en la ley y perseguir la consecución de una finalidad legítima, la restricción debe responder a una necesidad imperiosa (*"a pressing social need"*) en el marco de una sociedad democrática. Con esta condición el Tribunal se refiere, en esencia, al respeto del principio de proporcionalidad, que se proyecta, primero, en la necesidad estricta de la medida ejecutada, y, segundo, en su adecuación o congruencia con el objetivo perseguido por el Estado, *id est,* en la garantía de que no existe otra intervención menos intrusiva que permita la consecución de aquel. Este es, sin duda, el criterio de justificación más complejo o controvertido, y, a la vez, más determinante, pues en la gran mayoría de casos los otros dos requisitos, -previsibilidad legal y finalidad legítima-, son de fácil invocación por cualquier Estado parte del sistema convencional. El objetivo de preservar la seguridad nacional es un ejemplo paradigmático. Su legitimidad ha sido apreciada por el Tribunal incluso en aquellos casos en los que la restricción sobre la vida privada del individuo se produce a través de la intercepción de sus comunicaciones o utilización de sus datos personales sin siquiera mediar su autorización. Véase, por ejemplo, los asuntos *Klass and others v. Germany, Leander v. Sweden* o *Z. v. Finland* (*Ibidem*: pp. 37-39).

Con relación a este tercer criterio, -el de la "*pressing social need*"-, la principal problemática estriba en que en aquellos casos en los que apenas existe un estándar mínimo convencional, *p.ej.,* fenómeno religioso, seguridad y orden público o contexto digital y protección de datos, el Tribunal tiende a escudarse en la ambigua noción del margen de apreciación nacional para evitar analizar la necesidad de las injerencias realizadas por unos Estados soberanos que presuntamente actúan bajo los principios democrático y de *Rule of Law*. En efecto, cuanto menor es el consenso respecto a la delimitación de un derecho convencional, con mayor fundamento se siente la Corte para desentenderse del asunto y recurrir al margen de apreciación nacional, eludiendo con ello la

responsabilidad de decidir si la intromisión es necesaria o no. Esto provoca, a la postre, que la restricción de derechos fundamentales quede prácticamente impune, pues su juicio de legitimidad queda sujeto al margen de apreciación del Estado que precisamente ha sido acusado de la violación. Ello no hace más que degradar la eficacia del sistema convencional de garantía de derechos.

Tras sintetizar los criterios de ponderación a partir de los cuales los jueces de Estrasburgo pueden justificar, o no, las medidas restrictivas sobre los derechos convencionales de los arts. 8-11 CEDH, en general, y del art. 8 CEDH, en particular, conviene analizar la decisión adoptada por el Tribunal en *Glukhin v. Russia*. Este asunto es importante porque brinda a la Corte la oportunidad de pronunciarse sobre un conjunto de cuestiones de relevancia actual notable, como la implicación de los procesos de digitalización y globalización en la teoría de los derechos fundamentales, el clásico debate seguridad/privacidad, o el conflicto Estado liberal (democrático) *versus* Estado policial (autoritario). Este último asunto enlaza, a su vez, con la procedencia del Estado demandado, -Rusia-, así como con la actitud que muestra la Corte europea a la hora de rematar su fallo (párr. 90). A ello se hará especial alusión en las últimas páginas de este escrito.

III. Los riesgos inherentes al progreso tecnológico cuando éste cae en manos de un Estado autoritario. A vueltas con el asunto *Glukhin v. Russia*

Con el fin de protestar, de forma pacífica, contra el arresto del activista político *Kostantin Kotov*, el sr *Glukhin* decide manifestarse en solitario en el metro de Moscú con una imagen de cartón del detenido y una pancarta que decía: “You must be f**king kidding me. I’m Konstantin Kotov. I’m facing up to five years <<in prison>> under <<Article>> 212.1 for peaceful protests.” (apartado 7). Tan solo siete días después (30 de agosto de 2019), el Sr. *Glukhin* es arrestado en una de las estaciones del metro de la capital por haber incumplido el procedimiento establecido para la celebración de actos públicos conforme al Código nacional de infracciones administrativas. En concreto, su acusación se fundamenta en que la manifestación fue celebrada sin haber notificado previamente a las

autoridades competentes. Las fuerzas policiales tuvieron constancia de la manifestación a raíz de la visualización de una serie de imágenes compartidas en un canal público de *Telegram*. La unidad policial hizo varias capturas de las mismas y las almacenó en su base de datos junto con una serie de vídeos de la manifestación tomados por el sistema de videovigilancia (CCTV) instalado en el metro. Con apenas estas fuentes de información, las autoridades, a través de la realización de "actividades operativas de búsqueda" ("*operational-search activities"*), consiguen identificar al sr *Glukhin* y su dirección domiciliaria (apartado 11). Tras presentarse las fuerzas del orden en el domicilio y comprobar que no había nadie, en menos de una hora el demandante es detenido mientras viajaba en el metro después de haber sido rastreado y localizado por las cámaras instaladas en la estación pública[8].

Los tribunales condenan al acusado al pago de una multa de veinte mil rublos rusos con base a las pruebas aportadas por la policía: entre otras, las capturas realizadas del canal de *Telegram* y los vídeos procedentes de las cámaras de videovigilancia masiva del metro**.** El Sr. *Glukhin* recurre y alega la ilegalidad de las pruebas que sustentan su condena, pues el derecho nacional no ampara el empleo de técnicas de reconocimiento facial para captar y procesar datos biométricos en el marco de investigación de ilícitos administrativos, por ser aquella una tecnología demasiado intrusiva. De igual forma, el recurrente también denuncia la violación de su derecho a la libertad de expresión, pues la manifestación se realizó en solitario y de forma pacífica sin poner en peligro la salud pública (apartado 16). Tras agotar la vía jurisdiccional interna, Sr. *Glukhin* acude a los jueces de Estrasburgo en enero de 2020, a los que plantea que las diligencias de investigación a las que había sido sometido, así como la sanción administrativa que le había sido impuesta, vulneran sus derechos a la protección a la vida privada (art. 8 CEDH) y a la libertad de expresión y reunión (arts. 10 y 11 CEDH). Dadas las deficiencias procedimentales, también plantea violación del art. 6 CEDH.

[8]Apartado 12: "According to the applicant, at about 10 a.m. on 30 August 2019 the police anti-extremism unit went to his home while he was not there. At about 11 a.m. on the same day, he was arrested at an underground station. *The police allegedly told him that he had been identified by the facial recognition CCTV cameras installed in the Moscow underground"*. Énfasis añadido.

Respecto a la violación de los derechos políticos del demandante, la Corte valora toda la cuestión desde el prisma del art. 10 CEDH (apartado 47), haciendo hincapié en que los Estados cuentan con un ámbito de restricción especialmente estrecho cuando se trata de limitar el derecho a expresar la libre opinión sobre asuntos de relevancia pública. Dicho esto, procede a realizar el clásico "test de Estrasburgo". Así, tras confirmar que el arresto policial y la ulterior imposición de la multa administrativa implicaron una injerencia en el derecho a la libertad de expresión, el TEDH dictamina violación del art. 10 CEDH. Pese a admitir la prevención del desorden público como finalidad legítima, la Corte se muestra dubitativa en cuanto a la precisión o claridad con la que el derecho nacional regula y motiva la injerencia, y, en cualquier caso, deja claro que su aplicación en el caso concreto no es necesaria en una sociedad democrática (apartado 55). *Glukhin* incumple con una obligación administrativa de entidad menor, que además está regulada en el ordenamiento estatal de forma vaga e incoherente, lo que evidencia que su condena proviene de unas autoridades poco tolerantes y sedientas de control y castigo (apartado 56). El Estado ha restringido el derecho democrático estrella de forma desproporcionada e innecesaria, y a ello responde su condena (apartado 57).

Tras sentenciar, sin rodeos (apartados 49-57), la vulneración del art. 10 CEDH, la Corte se adentra con más detenimiento en valorar la compatibilidad del empleo de técnicas de reconocimiento facial con el derecho al respeto a la vida privada *ex.* art.8 CEDH, cuya concepción convencional es amplia y nada exhaustiva. El Tribunal no atribuye a la noción de vida privada un sentido estrictamente literal, es decir, no limita su significación al derecho a disfrutar de un riguroso "*inner cicle*" al margen de la sociedad. Al contario. El art. 8 CEDH acoge, también, el derecho a tener y dirigir una "vida social privada", y ampara, en consecuencia, las actuaciones realizadas en lugares públicos y/o en relación con otros sujetos (apartado 64). En ese sentido, la mera instalación de sistemas de videovigilancia en la vía pública no tiene por qué presentar deficiencias de legitimidad o de adecuación con el art. 8 de la Convención, más aún cuando con su despliegue se persigue la salvaguarda de la seguridad nacional y el orden público. Pueden, empero, aparecer injerencias problemáticas en relación con el

art. 8 CEDH cuando las imágenes son grabadas y almacenadas de forma sistemática para identificar e investigar a los sujetos, indistintamente de que dichos datos provengan del monitoreo rutinario de actividades y lugares públicos. Y ello porque la tutela del derecho a la protección de la propia imagen y de los datos de carácter personal, cuyo contenido abarca, entre otras cosas, la posibilidad de conocer sobre su procesamiento y utilización, deviene esencial para que el derecho al respeto a la intimidad y privacidad *ex.* art.8 CEDH quede, a su vez, plenamente garantizado (apartados 66, 67 y 75)[9]. En consecuencia, el procedimiento de obtención y disposición de datos personales por parte de los poderes públicos ha de estar regulado (previsto) en el derecho nacional, y venir acompañado de las suficientes garantías jurídicas que eviten cualquier tipo de abuso o arbitrariedad. En particular cuando la utilización de los datos tiene lugar en el marco de una investigación policial mediante el empleo de recursos tecnológicos cada vez más intrusivos y sofisticados. Y es que, como ya dejó claro la Corte en *S. and Marper v. the United Kingdom*: "The protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests" (apartado 75).

Tras traer a colación estas bases jurisprudenciales, la Corte identifica tres actividades con cuya realización las autoridades rusas han limitado o restringido el derecho al respeto a la vida privada de *Glukhin:* primero, mediante la obtención y almacenamiento de las capturas de las imágenes de *Telegram* y de las grabaciones de las cámaras del metro, a las que se les aplica técnicas de reconocimiento facial para identificar al demandante. Segundo, al recurrir a las cámaras del metro equipadas con sistemas de reconocimiento facial en tiempo real para localizar y arrestar al recurrente. Y, finalmente, al haber utilizado todas estas fuentes de datos biométricos como prueba para fundamentar la sanción administrativa (apartado 68). Pese a que las autoridades no reconocen

[9]Si bien el derecho a la protección a la vida privada y familiar *ex.* art.8 CEDH abarca, también, el derecho a la protección de datos de carácter personal, en la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE) ambos derechos se desdoblan en dos artículos diferentes pero inescindibles el uno del otro (arts. 7 y 8 CDFUE).

expresamente en sus informes el empleo de técnicas de reconocimiento facial para identificar, localizar y arrestar al recurrente, entre otras cosas, porque la legislación nacional no les obliga a registrar su utilización, tanto el sr *Glukhin* como la propia Corte lo dan por sentado. No en vano, aquellas apenas necesitaron dos días para identificar al demandante a partir de las capturas de *Telegram,* y solo una hora para localizarlo en el metro de la ciudad tras comprobar *in situ* que no se encontraba en su domicilio. Por otra parte, las instituciones rusas no hacen referencia alguna a ninguna otra estrategia o recurso que les hubiera permitido conseguir tal hallazgo de forma menos invasiva pero igual de eficaz (apartados 69-73)[10].

Confirmada la existencia de la injerencia, la Corte procede a valorar si ésta está o no justificada, es decir, si es legítima. Y ello lo hace enfatizando en el hecho de que sus estándares son especialmente exigentes en aquellos supuestos en los que los datos almacenados, además de servir para identificar y localizar al sujeto, también describen información de contenido sensible, como la que revela su orientación sexual, identidad étnica o ideología política. El uso y procesamiento de este tipo de datos exige una regulación clara y concreta acompañada de unas garantías mínimas, como la determinación de la duración del uso y almacenamiento de los datos, la categoría de sujetos que van a tener acceso a los mismos, o el establecimiento de unos procedimientos que aseguren su integridad, confidencialidad y posibilidad de destrucción, para evitar así cualquier tipo de abuso o arbitrariedad (apartados 76, 77, 82).

Dicho esto, es evidente que, en el caso concreto, Rusia no cumple con los mínimos exigidos para superar el “test de Estrasburgo”. Y ello pese a admitir

[10]Esta actitud de la Corte rememora a la asumida en *Klass v. Germany*. En este asunto el TEDH empatiza con las enormes dificultades a las que tiene que hacer frente el recurrente a la hora de probar el perjuicio directo ocasionado por la injerencia estatal cuando ésta tiene carácter secreto. La condición de víctima se fundamenta aquí en la mera existencia de una ley nacional que regula la adopción de las medidas restrictivas, sin que sea necesario probar que la misma le ha sido efectivamente aplicada. Esta postura irá siendo adoptada en numerosos casos posteriores relacionados con la afectación de derechos a consecuencia de políticas de control ejecutadas en nombre de la seguridad nacional. Véase, por ejemplo, el caso *Roman Zakharov v. Russia.* Siguiendo esta misma línea, así como la pautada, también, por la sentencia *Gaughran v. the United Kingdom,* basta con la posibilidad (razonable) de que las autoridades puedan aplicar tecnología de reconocimiento facial sobre las imágenes almacenadas para apreciar injerencia en el derecho a la protección a la vida privada; STEDH *Glukhin v. Russia, ob.cit;* apartado 72.

la finalidad legítima de la injerencia, *id est,* la prevención del crimen (párr. 84), o su previsión y regulación en la legislación nacional. En efecto, si bien el Decreto número 410, la Ley de Policía ("the Police Act") o el Código de Infracciones Administrativas ("Code of Addministrative Offences"; "the CAO"), atribuyen a la policía las competencias necesarias para investigar ilícitos administrativos mediante el procesamiento y análisis de datos personales (apartado 81), lo cierto es que dichas normas lo hacen de forma imprecisa e inconcreta. No en vano, el marco jurídico habilita a la policía a almacenar datos biométricos "en relación con la administración de justicia", lo que deja entrever que la habilitación opera, en realidad, para cualquier tipo de procedimiento judicial. Además, ni siquiera se concretan los objetivos que justifican el empleo de unas diligencias de investigación tan intrusivas, en qué tipo de casos deviene oportuno su recurso o los sujetos susceptibles de ser sometidos a las mismas. Tampoco se describe mecanismo alguno de supervisión y control en garantía de la independencia del procedimiento. En definitiva, concurre el requisito (formal) de la previsibilidad legal, pero la Corte duda de su calidad y seguridad (apartados 83 y 87)[11]. La apreciación de la violación del art. 8 CEDH depende, en esencia, del criterio referido a la "*pressing social need*" en el marco de una sociedad democrática.

Para pronunciarse sobre esta última cuestión, la Corte vuelve a las bases de las que parte el caso: la policía recoge y almacena unas imágenes y grabaciones del recurrente, -las primeras dispersas en la red y las segundas procedentes de las grabaciones de las cámaras de videovigilancia masiva del metro-, a las que aplica técnicas de reconocimiento facial para extraer y almacenar los datos biométricos de aquel. Ello le permite, primero, identificarlo, y, después, localizarlo y arrestarlo con la ayuda de las mismas cámaras equipadas con tecnología de reconocimiento facial en tiempo real. Se trata de restricciones especialmente invasivas e intrusivas, que revelan además información sensible en tanto que muestran al sujeto celebrando una manifestación de carácter político. En consecuencia, su "necesidad en una sociedad democrática" requiere de una motivación y justificación amplia y

[11]Apartado 87: "[..] The domestic law permits the processing of biometric personal data in connection with the investigation and prosecution of *any offence, irrespective of its nature and gravity*". Énfasis añadido.

exigente (apartado 86). En relación con esto último, el TEDH recalca la gravedad, ínfima, del ilícito por el que es condenado Sr. *Glukhin*: infracción administrativa consistente en incumplir con la obligación procedimental de notificación previa[12]. Nada más. Por otra parte, el empleo, generalizado en Rusia (apartado 40), de técnicas de reconocimiento facial para controlar, identificar, y, en su caso, arrestar a disidentes políticos, genera un indeseable *"chilling effect*" que degrada el contenido esencial de los derechos a la libertad de expresión y de asociación (apartado 88).

En suma, el empleo de técnicas de reconocimiento facial en diferido sobre las imágenes del demandante para identificarlo, junto con el ulterior recurso a técnicas de reconocimiento facial en tiempo real para localizarlo y arrestarlo, suponen una restricción sobre su derecho a la protección a la vida privada (art. 8 CEDH) que no responde a una necesidad social imperiosa en el marco de una sociedad democrática (apartados 89 y 91).

Al sentenciar, de forma tan contundente, las violaciones de los arts. 8 y 10 de la Convención, la Corte no aprecia la necesidad de valorar la posible afectación del art. 6 CEDH (apartado 92).

IV. ¿Hacia la normalización de los sistemas de reconocimiento facial?

A primera vista, la sentencia promete. Con ella la Corte se adentra en el estudio de los sistemas de videovigilancia masiva y su naturaleza proclive al abuso cuando éstos se ven perfeccionados por la Inteligencia artificial. Y, en particular, cuando se utilizan de la mano de técnicas de reconocimiento facial en tiempo real. Para que su empleo sea necesario en el marco de una sociedad democrática, el TEDH exige al Estado cumplir con un nivel de justificación elevado; el más elevado (apartado 86). La imposición convencional de un estándar de legitimidad amplio y exigente puede venir a arrojar luz en el seno de las instituciones de la UE, a día de hoy inmersas por conseguir la adopción de un marco normativo común sobre la Inteligencia artificial, en general, y las

[12] *Ibidem*: "In the assessment of the <<necessity in a democratic society>> of the processing of personal data in the context of investigations, the *nature and gravity of the offences in question is one of the elements to be taken into account* […]". Énfasis añadido.

técnicas de reconocimiento facial, en particular[13]. Ello iría en línea con lo establecido por el art. 6.3 TUE, que incorpora la jurisprudencia de la Corte al Derecho originario como Principios Generales de Derecho comunitario, o por el art. 52.3 CDFUE, que adscribe a los derechos plasmados, también, en el Convenio, el mismo sentido y alcance que les otorga este último, sin perjuicio de que en el orden comunitario se les pueda reconocer un nivel de protección más amplio (NERONI REZENDE, 2023).

La sentencia, sin embargo, más allá de la novedosa temática a la que responde, aporta más bien poco. Mas aun cuando de lo fallado se infiere el carácter legítimo de unas restricciones cuya aplicación, por sí sola, viola el contenido esencial de los derechos convencionales.

La Corte no resuelve ni con rotundidad, ni con precisión, si las interferencias resultantes del empleo de técnicas de reconocimiento facial son legítimas o ilegítimas. Antes bien, impone la existencia de un marco normativo claro que regule el alcance de su aplicación y que establezca, además, un sistema de garantías que evite cualquier tipo de arbitrariedad (apartado 82). El TEDH, por tanto, pone su centro de atención en prevenir el abuso por parte de los poderes públicos, así como en que el marco normativo sea transparente y accesible. De ahí, en principio, es posible inferir que su regulación y empleo, *per se*, es un recurso de restricción legítimo para los Estados (PALMIOTTO & MENÉNDEZ GONZÁLEZ, 2023: p. 4). En ese sentido, se puede decir que el Tribunal asume una posición similar, -pero no idéntica-, a la mostrada en sus decisiones sobre el carácter convencional de las políticas de intercepción masiva de comunicaciones y de retención de los datos derivadas de las mismas (NERONI REZENDE, 2023).

[13]En la noche del 8 de diciembre de 2023, el trílogo europeo consiguió alcanzar un acuerdo provisional sobre la propuesta relativa a las normas armonizadas en materia de inteligencia artificial; conocida como la ley de Inteligencia artificial (*AI Act*), que adoptará la forma de Reglamento. Con ello se acerca la conclusión de un arduo procedimiento legislativo que comenzaba en abril de 2021 con la iniciativa presentada por el Ejecutivo europeo: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52021PC0206 . Uno de los puntos clave de las negociaciones entre la Comisión europea, el Consejo de la UE y el Parlamento europeo ha sido, precisamente, el empleo de sistemas de identificación biométrica en tiempo real y en lugares públicos.

En efecto, en asuntos como *Big Brother Watch v. the United Kingdom* (I y II) o *Centrum för Rättvisa v. Sweden* la Corte tampoco niega, en abstracto, el carácter ilegítimo de este tipo de interferencias cuando se ejecutan frente a la amenaza terrorista. Ni siquiera en aquellos casos en los que se adoptan acuerdos de transmisión e intercambio de los datos con terceros países[14]. Y ello lo admite la Corte con rotundidad, esto es, de forma explícita y con carácter general. Nada que ver con la imprecisión de la que adolece la respuesta dada en *Glukhin* respecto a la tecnología de reconocimiento facial[15].

A la hora de enjuiciar la legitimidad (o no) de la obtención, procesamiento y utilización de datos biométricos a través del empleo de la tecnología de reconocimiento facial, la Corte sigue, en cambio, la senda pautada en *S. and Marper v. the United Kingdom*[16], reduciendo con ello el alcance de su resolución: "[…] The question is not whether the processing of biometric personal data by facial recognition technology *may in general* be regarded as justified under the Convention. *The only issue* to be considered by the Court is whether the processing of the applicant's personal data was justified under Article 8 § 2 of the Convention *in the present case*"[17]. En síntesis, el empleo de este tipo de

[14]Esta postura de los jueces de Estrasburgo sobre los acuerdos de transferencia intercontinental de datos deja bastante que desear si la comparamos con la asumida por el TJUE en *Schrems* (I) y *Facebook Ireland and Schrems* (II). O, también, en los asuntos *Digital Rights Ireland and Seitlinger and Others* y *Tele2 Sverige*. En estos últimos casos el TJUE recurre al principio de proporcionalidad para rechazar la obligación que los Estados imponen a los proveedores de servicios de comunicaciones electrónicas de retener y entregar datos personales a las fuerzas de seguridad nacionales. Aunque lo cierto, empero, es que esta última postura se ha visto relativizada en los casos *La Quadrature du Net and Others* y *Commissioner of An Garda Síochána,* en los que el Tribunal de Luxemburgo ha llegado a admitir la conservación indiscriminada de datos cuando ésta se realice para perseguir delitos especialmente graves y peligrosos para la seguridad nacional (REVENGA SÁNCHEZ, 2023: p. 251).

[15]Compárese, por ejemplo, el párr. 85 de la sentencia *Glukhin* con el párr. 314 de la sentencia *Big Brother Watch* (I). Este último establece lo siguiente "[..] in *Weber and Saravia* and *Liberty and Others* the Court accepted that bulk interception regimes did not *per se* fall outside this margin. Although both of these cases are now more than ten years old, given the reasoning of the Court in those judgments and in view of the current threats facing many Contracting States (including the scourge of global terrorism and other serious crime, such as drug trafficking, human trafficking, the sexual exploitation of children and cybercrime), advancements in technology which have made it easier for terrorists and criminals to evade detection on the Internet, and the unpredictability of the routes via which electronic communications are transmitted*, the Court considers that the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States' margin of appreciation".* Énfasis añadido.

[16]En este asunto se analizaba si la conservación de las huellas dactilares, muestras celulares y perfiles de ADN de los recurrentes estaba justificada a la luz del art. 8.2 CEDH.

[17]Párr. 85. Énfasis añadido.

tecnología vulnera el art. 8 CEDH bajo las circunstancias, específicas, del caso concreto. Esta actitud de "*self-restraint"* es coherente con la naturaleza institucional de la Corte, pues su jurisprudencia fue originariamente concebida para enjuiciar las actuaciones lesivas de los derechos convencionales caso a caso. Lo que no ha sido óbice, por otra parte, para que la misma Corte, en más de una ocasión, haya asumido un rol mucho más proactivo, (o por lo menos no tan impreciso), a la hora de pronunciarse sobre restricciones que claramente afectaban derechos convencionales. Así ha ocurrido, de hecho, en diversos asuntos relacionados, también, con el empleo de técnicas de vigilancia masiva en nombre de la seguridad nacional (*Ibidem*). Véase, por ejemplo, los casos *Klass v. Germany, Roman Zakharov v. Russia*[18], *Szabó and Vissy v. Hungary, Big Brother Watch and others v. the United Kingdom* (I y II)[19], *Centrum för Rättvisa v. Sweden* o *Ekimdzhiev and Others v Bulgaria*.

En el apartado 85 de la sentencia la Corte se muestra ambigua y ambivalente. Por una parte, ésta lamenta el predomino actual de la crisis global "securitaria" y condena las amenazas procedentes de los grupos terroristas y redes de crimen organizado, lo que la lleva a admitir su persecución a través de mecanismos de seguimiento masivos y sofisticados, dentro de los cuales se colige que se encuentran las tecnologías de reconocimiento facial. Pero, por otra parte, los jueces de Estrasburgo tampoco dejan pasar por alto su naturaleza intrusiva y tendente al abuso. De ahí la necesidad de delimitar, con la suficiente precisión y claridad, su ámbito y fundamento de ejecución.

El problema, no obstante, es que la Corte construye su decisión de no convencionalidad a partir de los presupuestos del caso concreto[20]. Esto es, circunscrita a un contexto político-jurídico muy peculiar, arraigado en un Estado que ni siquiera es ya parte del sistema convencional de derechos europeo.

[18]Sobre este caso véase a DE HERT & CRISTOBAL BOCOS (2015): https://strasbourgobservers.com/2015/12/23/case-of-roman-zakharov-v-russia-the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/.

[19]WATT (2021) realiza un interesante análisis de la saga jurisprudencial *Big Brother Watch v. the United Kingdom* en *https://strasbourgobservers.com/2021/06/28/much-ado-about-mass-surveillance-the-ecthr-grand-chamber-opens-the-gates-of-an-electronic-big-brother-in-europe-in-big-brother-watch-v-uk/*. De la misma autora y con fecha más reciente (2022) también puede consultarse: https://verfassungsblog.de/os6-privacy-vs-security/.

[20]Apartado 89: "*In such circumstances*, the use of facial recognition technology […] did not correspond to a <<pressing social need>>." Énfasis añadido.

Precisamente es en la procedencia del Estado demandado donde la Corte, en tanto que entidad dedicada, exclusivamente, a la tutela supraestatal de derechos, parece que pierde el foco. El caso responde a una temática muy concreta: la afectación de derechos en aras de preservar la seguridad y el orden público nacional. Con la particularidad de que dicha afectación se produce a consecuencia de un conjunto de restricciones tan intrusivas como eficaces para investigar y prevenir ilícitos. En ese sentido, el contexto actual de globalización tecnológica exigía una sentencia clara y garantista. Nada más lejos de la realidad.

La sentencia es estimatoria, sí. Confirma la violación del art. 8 CEDH al haber empleado Rusia tecnología de reconocimiento facial de forma desproporcionada. Mas esa reprobación se limita a las circunstancias específicas en las que ésta se utiliza por el Estado ruso, país que, por razones obvias, no cumple con los estándares convencionales mínimos que sí prevalecen en el resto de Estados del sistema. Luego, ese rechazo al empleo del reconocimiento facial tanto en diferido como en tiempo real, y cuya proporcionalidad, en cualquier caso, es cuanto menos que cuestionable, no será fácil de extrapolar a las futuras demandas que están por caer ante el TEDH y que no serán tan "fáciles" de resolver. No en vano, no son pocos los Estados parte cuyas fuerzas policiales han utilizado sistemas de identificación biométrica con fines tanto preventivos, como persecutorios de delitos "menores"[21]. Por ello, en lugar de (auto)restringir el alcance de su decisión (apartado 85), la Corte debería haber sentenciado en abstracto, para así esclarecer cuán de legítimo resultaría el empleo de una tecnología intrínsecamente intrusiva a manos de un Estado realmente democrático y garante de derechos. O, de resultar

[21]Así, por ejemplo, el 4 de septiembre de 2019 el Alto Tribunal de Justicia de Inglaterra y Gales se pronunció sobre el uso masivo de sistemas de reconocimiento facial automático en tiempo real por las autoridades policiales galesas. La sentencia responde a la ejecución del proyecto piloto "*Automated Facial Recognition Locate"*, que consistía en el empleo generalizado, durante la celebración de una serie de eventos determinados, *p.ej.,* la final de la *Champions League*, de sistemas de videovigilancia con el fin de capturar imágenes del público asistente y compararlas en tiempo real con otras imágenes almacenadas en los archivos policiales. El caso lo analiza con detalle IZQUIERDO CARRASCO (2020: p.87). También es destacable que la policía italiana de la localidad de Brescia pudiera detener a dos sospechosos de haber asaltado una casa en la provincia de Lombardía gracias al empleo de sistemas de identificación biométrica (ROMANDINI, 2018).

convencional su recurso, haber dictaminado en qué casos y bajo qué circunstancias.

En definitiva, se echa en falta la definición de un conjunto de orientaciones generales, que, más allá de hacer referencia a la naturaleza y gravedad de la infracción (apartado 87), hubiera dispuesto, con suficiente rigor, un marco mínimo de proporcionalidad según el cual el empleo del reconocimiento facial por los Estados estaría justificado. Así, como sugieren PALMIOTTO & MENÉNDEZ GONZÁLEZ (2023: p. 5), el Tribunal podría haber señalado qué tipo de delitos, dejando fuera, lógicamente, ilícitos administrativos como los del caso analizado, pueden ser investigados o prevenidos a través de las técnicas de identificación facial.

En relación con esta última cuestión, la iniciativa normativa de la Comisión europea propone la regulación de los sistemas de Inteligencia artificial conforme a cuatro niveles de riesgo según el peligro que su empleo entrañe para los derechos de los ciudadanos, de tal manera que, a mayor peligro, mayor riesgo, y, por tanto, mayor escrutinio y más formalidades. Así, bajo el peldaño de "riesgo inadmisible", que incluye las técnicas prohibidas de forma terminante[22], los sistemas de reconocimiento biométrico se encuentran en el escalón inmediatamente inferior; el de "riesgo alto". Ello implica que la Comisión, respaldada por el Consejo, prohíbe, con carácter general, el empleo de sistemas de identificación facial en tiempo real en lugares públicos con fines de aplicación de la ley[23], salvo en aquellos casos cuyo recurso sea "estrictamente necesario", *p.ej.,* para prevenir una amenaza específica, importante e inminente para la vida o la seguridad física de las personas o de un atentado terrorista (art. 5.1 (d) (ii)). En defensa del TEDH, se podría decir que el criterio comisario de lo "estrictamente necesario" evoca a los estándares convencionales de la "*pressing social need"* o "*highest level of justification*" (PALMIOTTO & MENÉNDEZ GONZÁLEZ, 2023: p. 4). Pero, en cualquier caso, son parámetros demasiado ambiguos, bajo

[22]Entre otras, aquellos sistemas de inteligencia artificial capaces de manipular el comportamiento humano y fomentar la violencia; *p.ej.,* un juguete con asistencia de voz que pueda animar a los menores a realizar actuaciones peligrosas (CASTELLANOS CLARAMUNT, 2023: p. 269).
[23]Por "aplicación de la ley" se entiende aquellas actividades realizadas para prevenir, investigar, detener o enjuiciar infracciones penales o ejecutar sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública; art. 3 (41).

los cuales sigue quedando en el aire la posibilidad de que este tipo de tecnología se acabe convirtiendo en una herramienta "securitaria" más normal que excepcional.

Este era el paradigma hasta diciembre de 2023, momento en el que se producen novedades importantes en el contexto de la Unión Europea. En efecto, si bien el acuerdo alcanzado tras la conclusión de las negociaciones del trílogo europeo da la victoria a la línea marcada por el Consejo y la Comisión, en el sentido de que se opta por la prohibición general de los sistemas de identificación biométrica pero matizada por algunos casos de excepcionalidad vinculados a la seguridad nacional, lo cierto es que, en comparación con la inicial propuesta de la Comisión, el Parlamento ha conseguido imponer un mayor conjunto de salvaguardias y restricciones para el uso de la tecnología de reconocimiento facial. Así, la identificación biométrica en diferido o "post-remota" se empleará, solo, para la búsqueda de una persona condenada o sospechosa de haber cometido un delito grave. Asimismo, -y aquí viene lo más destacable-, el empleo del reconocimiento facial en vivo se limitará al conjunto de delitos graves que se detallan, específicamente, en la propia regulación; *et.al.,* terrorismo, trata de seres humanos, violación o secuestro (IGLESIAS FRAGA, 2023).

Resulta evidente que el compromiso asumido por las instituciones de la UE dista de la actitud evasiva mostrada por el TEDH en *Glukhin.* Así, este último tampoco considera oportuno pronunciarse sobre las diferentes implicaciones que conlleva el empleo de sistemas de reconocimiento facial en diferido, -en los que resulta factible delimitar o discriminar el número de sujetos sometidos a control-, y en tiempo real, cuya ejecución, por el contrario, lleva aparejada un inevitable seguimiento masivo y generalizado de los ciudadanos. Esta negligencia acrecienta, más si cabe, el carácter incongruente e impreciso de la sentencia. No se puede imponer, bajo el pretexto del requisito de la "calidad de la ley", que el ordenamiento nacional determine los sujetos susceptibles de verse sometidos a este tipo de sistemas cuando su empleo, por lo menos cuando éste tiene lugar en tiempo real, requiere, en todo caso y de forma ineludible, de una videovigilancia constante, masiva e indiscriminada de la ciudadanía (PALMIOTTO & MENÉNDEZ GONZÁLEZ, 2023: p. 5).

Caso omiso, por cierto, hace la Corte a la cuestión de si es legítimo o no que las autoridades utilicen y almacenen imágenes procedentes de las redes sociales (*Telegram*). Este asunto tampoco es baladí. Por mucho que la disponibilidad de aquellas sea pública, el foco de atención ha de residir en si ha sido el propio sujeto el que ha publicado las imágenes, pues con razón a esto último sus expectativas de privacidad habrán de ser más o menos amplias. En la sentencia no se especifica si las imágenes de *Telegram* fueron o no publicadas por el sr *Glukhin*, pero, indistintamente, una mera aclaración por parte de la Corte podría haber contribuido a frenar la sensación de hipervigilancia continua que se extiende entre las ciudadanías europea y mundial (RIDAURA MARTÍNEZ, 2023: p. 276, PALMIOTTO & MENÉNDEZ GONZÁLEZ, 2023: p. 6).

En definitiva, en lugar de ejercer como un auténtico tribunal de derechos comprometido por definir un estándar garantista en torno a la dialéctica derechos-seguridad en el contexto tecnológico, la Corte prefiere no inmiscuirse en una cuestión compleja y controvertida, respecto a la que Estados e instituciones mantienen una actitud divergente. Así lo demuestran las posiciones mantenidas por los organismos de la UE en el marco de negociaciones para aprobar La ley de Inteligencia artificial, durante el cual, como ya se ha hecho alusión, la Comisión y el Consejo promueven la regulación del reconocimiento facial en tiempo real como recurso excepcional y susceptible de ser empleado cuando resulte “estrictamente necesario”, mientras que el Parlamento lo considera contrario a los valores europeos, y por ello pugna por prohibir, en todo caso, su ejecución en espacios públicos (NERONI REZENDE, 2023). Y es que, como se desprende de lo afirmado por RIDAURA MARTÍNEZ (2023: p. 277), los peligros inherentes a la tecnología del reconocimiento facial transcienden el clásico dilema seguridad-privacidad, pues su aplicación redunda en la afectación de una gama de derechos amplia y diversa: intimidad, propia imagen, protección de datos personales, libertad de expresión o presunción de inocencia. La regresión de este último derecho es significativa. No en vano, es evidente que la Inteligencia artificial ha revolucionado el método de trabajo tradicionalmente seguido por las autoridades para prevenir la comisión de ilícitos. Hasta ahora, éstas construían un marco de investigación sobre indicios, y tras quedar estos

verificados, se actuaba en consecuencia: restringiendo derechos. Orden congruente con el derecho a la presunción de inocencia. Con el advenimiento de la tecnología de reconocimiento facial automático y su aplicación en tiempo real, las fuerzas del orden consiguen una valoración sobre la correspondencia entre dos imágenes faciales. En caso de darse esta última, cualquier individuo es susceptible de ser trasladado a las instancias policiales para confirmar dicha correspondencia, o, incluso, para interrogarlo e investigarlo directamente. Los ciudadanos quedan así sometidos a unas injerencias indeseadas y desproporcionadas, así como la eficacia de su derecho a la presunción de inocencia reducida prácticamente a la nada (IZQUIERDO CARRASCO, 2020: p. 94). El arresto de Sr. *Glukhin* es claro ejemplo de ello.

Mención aparte merecen los perjuicios discriminatorios que la simple puesta en marcha de este tipo de sistemas supone para ciertos colectivos minoritarios y/o sujetos vulnerables. Los sistemas de identificación biométrica operan a través de una serie de algoritmos matemáticos que se encargan de estigmatizar y clasificar a los sujetos conforme a criterios como el género o la identidad étnica, de manera que el mayor número de errores suele originarse con las mujeres y/o sujetos de piel oscura, por ser estos "más difíciles" de identificar que los hombres de tez blanca (RIDAURA MARTÍNEZ, 2023: pp. 277-278). En relación con esto último, no está de más recordar que estos "sesgos algorítmicos" se derivan de las prejuicios y decisiones tomadas por los seres humanos que intervienen en su proceso de creación (CASTELLANOS CLARAMUNT, 2023: pp. 278-279).

En definitiva, sobre *Glukhin v. Russia* planea un conjunto de amenazas con suficiente potencial como para poner en tela de juicio las bases de un sistema que se empeña en no avanzar conforme lo hacen la sociedad y el mercado. La Corte, pese a ser consciente de ello, "se lava las manos". Mas sí que decide, en cambio, proclamar una guerra de valores contra Rusia: "[…] the Court concludes that the use of highly intrusive facial recognition technology in the context of the applicant exercising his Convention right to freedom of expression is incompatible *with the ideals and values of a democratic society governed by the rule of law, which the Convention was designed to maintain and*

promote. […]"[24]. Es decir, si algo queda claro tras el fallo pronunciado en *Glukhin,* es que los valores constitucionales europeos, esto es, el principio democrático y de *Rule of Law,* son intocables. Y que todo Estado que no comulgue con ellos incumple con los estándares de la Convención. Ahora bien, la Corte no debe olvidar que entre dichos valores europeos se encuentra, también, la protección de los derechos humanos, cuya garantía efectiva depende, en gran medida, de su compromiso y responsabilidad. Es por ello por lo que aquella debería rechazar, sin reticencias y con carácter general, cualquier injerencia susceptible de erosionar, *per se,* la esencia irreductible de los derechos de la Convención. Entre ellos y en particular, el derecho a la privacidad e individualidad. No en vano, recuérdese que este último derecho, junto con el de la libertad o los derechos de carácter procedimental, todos ellos invocados, por cierto, por Sr. *Glukhin* (arts. 8, 10, 11 y 6 CEDH), representa la quintaesencia del constitucionalismo liberal del que emerge la Europa que conocemos hoy.

Con esta afirmación no se pretende sacralizar el derecho a la privacidad, ni enfrentarlo al principio de garantía de la seguridad nacional. Al contrario. Lo que se pretende, más bien, es resaltar que la relación seguridad-privacidad no es de carácter conflictual (MARTÍN Y PÉREZ DE NANCLARES, 2008: p. 220), sino de necesidad. Que ambos conceptos se retroalimentan y que uno depende del otro. Las exigencias de seguridad colectiva no pueden servir a los Estados como pretexto para vaciar de contenido el derecho a la privacidad de sus ciudadanos. Como la propia Corte indica en *Roman Zakharov v. Russia*, no se puede abogar por la seguridad de la democracia mientras ésta se destruye[25]. Y en ese sentido, no son pocas las preguntas que se nos plantean: ¿De verdad no se puede garantizar la seguridad nacional a través de una tecnología que no sea tan lesiva de derechos?, ¿es realmente eficaz la tecnología de reconocimiento facial?, ¿vale la pena apostar por una promesa de mayor seguridad a costa de una pérdida indiscriminada de privacidad? (VELASCO, 2023).

[24]Apartado 90. Énfasis añadido.
[25]"[…] In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, […]"; STEDH (Gran Sala), *Roman Zakharov v. Russia,* 04/12/15, apartado 232.

Lo ideal es que las respuestas a todas estas preguntas quedaran fijadas en las normas, pues con ello se acabaría con la necesidad de depender de la interpretación de los tribunales. A este respecto, los recientes avances alcanzados en el seno de la Unión Europea representan un atisbo de esperanza. Mas tampoco deberíamos pecar de un exceso de optimismo. Primero porque según se desprende de los acuerdos alcanzados tras el trílogo europeo, la propuesta de prohibición absoluta de la vigilancia biométrica masiva, ampliamente exigida por la sociedad civil[26], parece haber quedado definitivamente rechazada. Y, segundo, porque la entrada en vigor del Reglamento en cuestión dista aún de producirse a expensas de alcanzarse, todavía, el visto bueno definitivo del Consejo y Parlamento[27].

En tanto esto último sucede, esperemos que la Corte europea de derechos, con la ayuda del TJUE, asuma y aprenda de los errores cometidos en *Glukhin,* para que así, en los futuros casos por venir, el carácter desproporcionado del empleo, (aunque sea excepcional), de cualquier medida que atente, *per se*, contra la esencia mínima de los derechos fundamentales quede libre de toda duda. De lo contrario, es la Europa de los derechos y de la democracia la que estará en peligro.

[26]Véase, por ejemplo, la iniciativa promovida por el movimiento *reclaimyourface:* Global statement: Stop facial recognition surveillance now! Accesible en: https://edri.org/wp-content/uploads/2023/09/Global-statement-Stop-facial-recognition-now.pdf.

[27]Desde una perspectiva basada, rigurosamente, en la plena garantía de derechos fundamentales, lo cierto es que los precedentes normativos existentes en la UE con relación a la identificación biométrica tampoco son demasiado alentadores. Basta recordar, por ejemplo, el Reglamento nº. 603/2013 relativo a EURODAC, que permite la aplicación de la biometría en el ámbito de asilo como recurso de los Estados para obtener información exacta sobre la identidad de los solicitantes a través de su huella dactilar, o la ulterior propuesta de Reglamento EURODAC, que ligada, en particular, con este último, y, en general, con el Pacto sobre Migración y Asilo, plantea la Comisión el 4 de mayo de 2016, y la cual se encuentra ya acordada políticamente. Esta propuesta comisaria, conocida como PRE, dispone un conjunto de medidas que vendrán, sin lugar a dudas, a mejorar la eficiencia del sistema EURODAC de cara a los no pocos problemas a los que se enfrenta el Sistema Europeo Común de Asilo en su conjunto. Entre dichas medidas, destacan, *et.al*: la rebaja de la edad de la toma de los datos biométricos, la ampliación del período de conservación de los datos, o la simplificación del procedimiento de acceso a los mismos por parte de las fuerzas y cuerpos de seguridad. Ello tendrá lugar, empero, a costa de la degradación de los derechos de los solicitantes de protección internacional, y en concreto, de su derecho a la privacidad y protección de datos personales. Lo que encuentra justificación, como era de esperar, en la salvaguarda de la seguridad interna de los Estados, *a priori* amenazada a raíz de las deficiencias asociadas al sistema vigente (Reglamento nº. 603/2013); las cuales han dado lugar a que las identidades de una cantidad masiva de migrantes permanezcan invisibles o indeterminables ante las instituciones y bases de datos europeas. Esta cuestión es analizada con detalle por VIGURI CORDERO (2021, pp: 289-295).

V. Bibliografía

CASTELLANOS CLARAMUNT, J. (2023). *Sobre los desafíos constitucionales ante el avance de la inteligencia artificial. Una perspectiva nacional y comparada,* Revista de Derecho Político, Nº. 118, pp. 261-287. Accesible en: https://doi.org/10.5944/rdp.118.2023.39105

DE HERT, P., & CRISTOBAL BOCOS, P. (2015). *Case of Roman Zakharov v. Russia: The Strasbourg follow up to the Luxembourg Court's Schrems Judgment.* En Strasbourg Observers. Accesible en: https://strasbourgobservers.com/2015/12/23/case-of-roman-zakharov-v-russia-the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/

IGLESIAS FRAGA, A. (9 de diciembre de 2023). *Análisis de la ley europea de inteligencia artificial: pionera en el mundo, pero con rebajas en las prohibiciones*. Accesible en: https://www.elespanol.com/invertia/disruptores-innovadores/politica-digital/europa/20231209/analisis-ley-europea-inteligencia-artificial-pionera-mundo-rebajas-prohibiciones/815918401_0.html

IZQUIERDO CARRASCO, M. (2020). *La utilización policial de los sistemas de reconocimiento facial automático*, IUS ET VERITAS: Revista de la Asociación IUS ET VERITAS, Nº. 208, pp. 86-103. Accesible en: https://doi.org/10.18800/iusetveritas.202001.004

MARTÍN Y PÉREZ DE NANCLARES, J. (2008). *Respeto de la vida privada y familiar.* En MANGAS MARTÍN, A., GONZÁLEZ ALONSO, L.N, (coords.) Carta de los derechos fundamentales de la Unión Europea: comentario artículo por artículo. (pp. 223-243), Fundación BBVA.

NERONI REZENDE, I. (2023) *Glukhin and the EU regulation of facial recognition: Lessons to be learned?* En European Law Blog. Accesible en: https://europeanlawblog.eu/2023/09/19/glukhin-and-the-eu-regulation-of-facial-recognition-lessons-to-be-learned/

PALMIOTTO, F. & MENÉNDEZ GONZÁLEZ, N. (2023). *Facial recognition, technology, democracy and human rights.* En Computer Law & Security Review, Volume 50. Accesible en: https://doi.org/10.1016/j.clsr.2023.105857

PÉREZ DE LOS COBOS ORIHUEL, F. (2018). *El derecho al respeto de la vida privada: los retos digitales, una perspectiva de Derecho comparado.* Servicio de Estudios del Parlamento Europeo, Bruselas. Accesible en: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/628261/EPRS_STU(2018)628261_ES.pdf

Propuesta del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. Bruselas, 21.4.2021 COM (2021) 206 final 2021/0106 (COD). Accesible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52021PC0206

RECLAIMYOURFACE, *GLOBAL STATEMENT: STOP FACIAL RECOGNITION SURVEILLANCE NOW! ACCESIBLE* EN: HTTPS://EDRI.ORG/WP-CONTENT/UPLOADS/2023/09/GLOBAL-STATEMENT-STOP-FACIAL-RECOGNITION-NOW.PDF

REVENGA SÁNCHEZ, M. (2016). El derecho a la intimidad: un derecho en demolición (y necesitado de reconstrucción). En Asociación de Letrados del Tribunal Constitucional (coord..), *El derecho a la privacidad en el nuevo entorno tecnológico: XX Jornadas de la Asociación de Letrados del Tribunal Constitucional,* pp. 71-98, Madrid, Tribunal Constitucional-CEPC.

— (2023). El gran hermano ante Estrasburgo. En RIDAURA MARTÍNEZ, Mª. J. (dir.) *Retos para la seguridad,* Valencia, Tirant lo Blanch, pp. 247-266.

ROMANDINI, M. (27 de septiembre de 2018). *Come (non) funziona il Sistema Sari di riconoscimiento facciale.* Accesible en: https://www.wired.it/attualita/tech/2018/09/27/sari-riconoscimento-facciale/

RIDAURA MARTÍNEZ, Mª. J. (2023). El uso de cámaras de reconocimiento facial por empresas privadas de seguridad. En Ridaura Martínez, Mª. J. (dir.) *Retos para la seguridad,* Valencia, Tirant lo Blanch, pp. 267-313.

VELASCO, L. (17 de diciembre de 2019). *Gobernar la inteligencia artificial: el reconocimiento facial.* Accesible en: https://agendapublica.elpais.com/noticia/13835/gobernar-inteligencia-artificial-reconocimiento-facial

VIGURI CORDERO, J.A. (2021). *Seguridad y protección de datos en el sistema europeo común de asilo,* Valencia, Tirant lo Blanch.

WATT, E. (2021). *Much ado about mass surveillance -The ECTHR Grand Chamber "Opens the gates of an electronic "Big Brother" in Europe" in Big Brother Watch v. UK.* En Strasbourg Observers. Accesible en: https://strasbourgobservers.com/2021/06/28/much-ado-about-mass-surveillance-the-ecthr-grand-chamber-opens-the-gates-of-an-electronic-big-brother-in-europe-in-big-brother-watch-v-uk/

— (2022). *The legacy of the privacy versus security narrative in the ECtHR's jurisprudence.* En Verfassungsblog on Matters Constitutional. Accesible en: https://verfassungsblog.de/os6-privacy-vs-security/