

د. أحمد رجب صميده

دكتوراه في القانون العام – جامعة بني سويف
قاضي بمجلس الدولة المصري

الحماية القانونية للبيانات الحيوية في البيئة الرقمية: دراسة تحليلية نقدية في ضوء قانون الذكاء الاصطناعي في الاتحاد الأوروبي

■ المراسلة: د. أحمد رجب صميده

دكتوراه في القانون العام – جامعة بني سويف
قاضي بمجلس الدولة المصري

■ معرف الوثيقة الرقمي (DOI): jolets.v5i1.228/10.54873

ar.sd777@gmail.com

Ahmed011129@law.bsu.edu.eg

■ البريد الإلكتروني

■ نسق توثيق البحث

أحمد رجب صميده

الحماية القانونية للبيانات الحيوية في البيئة الرقمية: دراسة تحليلية
نقدية في ضوء قانون الذكاء الاصطناعي في الاتحاد الأوروبي
المجلد الخامس، العدد الأول، أبريل ٢٠٢٥

ملخص الدراسة

إنَّ استخدام تكنولوجيا القياس الحيوي – في الحالات التي يتمُّ فيها تطويرها ونشرها بشكلٍ مسنؤل - يُحقِّق العديدَ من الفوائد في المجالات المختلفة؛ مثلَّ الأمن والرعاية الصحيَّة، ومع ذلك؛ فقد يترتَّب على استخدامها انتهاكٌ للحقِّ الأساسي في الخصوصية، لذا تسعى هذه الدراسة إلى التَّعرُّف على بيانات القياس الحيوي، وبيان صُورها، استكشاف المخاطر المُرتبطة بنشر هذه التكنولوجيا بشكلٍ عامٍّ؛ وعلى الأخص تلك المتَّصلة بالحق في خصوصيَّة البيانات الشخصية، مع استعراض الأساليب والآليات التي يُوقِّرها «قانون الذكاء الاصطناعي» في الاتِّحاد الأوروبي لتلافي هذه المخاطر، وبيان مدى كفايتها في تحقيق الحماية الفعَّالة لتلك البيانات، وصولاً إلى نهجٍ قانوني يسعى إلى الموازنة بين ضرورة تشجيع الابتكار، وحماية الحقوق الفرديَّة

كلمات مفتاحية: بيانات القياس الحيوي، قانون الذكاء الاصطناعي، الحق في الخصوصية، اللائحة العامَّة لحماية البيانات، أنظمة الذكاء الاصطناعي، البيانات الشخصية، التحول الوظيفي

Abstract

Biometric technology, when developed and used responsibly, offers considerable benefits in various fields such as security and healthcare. Nevertheless, its deployment can significantly threaten the fundamental right to privacy. This study reveals to identify Bio-metric data and its manifestations, examining the risks associated with the general deployment of this technology, particularly those related to data protection rights. It further reviews the methods and mechanisms provided by the European Union's "Artificial Intelligence Act" to mitigate these risks, and its adequacy in achieving effective protection of that data, ultimately striving for a legal framework that aims to balance the necessity of encouraging innovation with the protection of individual rights.

Keywords: Biometric data, Artificial Intelligence Act, Right to Privacy, General Data Protection Regulation, (AI) systems, Personal data, Function creep.

إنَّ استخدام تقنيَّات القياس الحيوي لا يُعدُّ أمرًا مُستَحْدَثًا؛ فقد أشارت الدلائل لاستخدامها في الصين إبَّان القرن الرابع عشر^(١)، وقد بدأ استخدام تلك البيانات- آليًا- في الستينيَّات من القرن الماضي، وبدأت في النمو في التسعينيات، ويتمُّ استخدامها حاليًّا على نطاقٍ واسعٍ؛ لسببين رئيسيين: السبب الأول: المخاوف والاعتبارات الأمنيَّة؛ أما الثاني: فيتعلَّق بالفرص التي تُوفِّرُها تلك التقنيَّات في التَّعرُّف على الهويَّة البشريَّة، وتوثيقها عن طريق الخصائص الفريدة للأجسام البشريَّة^(٢).

وفي الوقت الحالي، تُستخدَم أنظَمَة القياس الحيوي في العديد من جوانب الحياة اليوميَّة، مُدَمَّجَةً مع تقنيَّات الذكاء الاصطناعي في ميزات؛ مثل هويَّة الوجه "Face-ID" على الهواتف الذكيَّة والمراقبة الآليَّة التي تُعدُّ أحد أكثر الأمثلة شيوعًا؛ وهو ما يحقِّق العديد من الفوائد العمليَّة، ولكنه - في الوقت ذاته- قد يُؤدِّي أيضًا إلى خُلُق العديد من التَّحديات المتعلِّقة بالخصوصيَّة والمراقبة الجماعيَّة المُفرطة، وحماية البيانات الشخصيَّة؛ الأمر الذي يُؤكِّد الحاجة إلى المزيد من النِّظَم والإشراف على هذه الأنظَمَة

وقد أصدر الاتحاد الأوروبي- بتاريخ ١٢ يوليو من عام ٢٠٢٤- قانون «الذكاء الاصطناعي»^(٣)؛ الذي يُعدُّ أوَّل إطار قانونيٍّ على الإطلاق للذكاء الاصطناعي، الذي قد يتضمَّن علاجًا مناسبًا لتلك التَّحديات؛ لذا تسعى هذه الدراسة إلى التَّعرُّف على بيانات القياس الحيوي وصُورها المختلفة، وبيان كفيَّة استخدام أنظَمَة التَّعرُّف الحيوي، وتطبيقاتها المُتعدِّدة، بالإضافة إلى التَّحديات الناجمة عن نشر التقنيَّات المُرتبطة بتكنولوجيا القياس الحيوي على الحقوق الفرديَّة؛

(1) Fingerprints were used by Chinese merchants to settle business transactions; fingerprints and footprints were used by parents to differentiate children.

« استخدم التجار الصينيون بصمات الأصابع لتسوية المعاملات التجارية، كما استخدمها أيضًا الآباء، بالإضافة إلى آثار الأقدام؛ للتمييز بين الأبناء.»

Yong Liu, Bio-privacy: Legal Challenges for Privacy Regulations of Biometric Identification and Authentication (2010) 3.

(2) المرجع السابق، ص1

(3) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689 accessed 31 May 2025

وخاصةً الحق في خصوصية البيانات الشخصية؛ وذلك في الأماكن التي يُتاح الوصول إليها بشكل عام؛ مُبَيَّنًا التدابير التي تَضُمُّهَا «قانون الذكاء الاصطناعي» في الاتحاد الأوروبي لحماية الحق في خصوصية البيانات الشخصية في سياق هذه التكنولوجيا؛ لمعرفة ما إذا كان قانون الذكاء الاصطناعي للاتحاد الأوروبي يُعَدُّ إطارًا قانونيًا كافيًا لتنظيم هذه المصالح المتعارضة

إشكالية البحث:

تتمثل مشكلة البحث في تساؤل مفاده: ما الطرق التي يُمكن من خلالها تحقيق الموازنة بين ضرورة تشجيع الابتكار المرتبط بتطور تقنيات القياس الحيوي وحماية الحق في خصوصية البيانات الشخصية؟ وينبثق منه عدة تساؤلات فرعية:

ما هو المقصود ببيانات القياس الحيوي، وما هي الصور التي تتخذها تلك البيانات؟

ما هو المقصود بأنظمة القياس الحيوي، وما هي طريقة عملها، تطبيقاتها المتعددة؟

ما هي المخاطر المرتبطة بنشر تكنولوجيا القياس الحيوي على الحقوق الفردية وخاصة الحق في خصوصية البيانات الشخصية؟

ما هي الأساليب والأليات التي وفرها «قانون الذكاء الاصطناعي» في الاتحاد الأوروبي لتلافي المخاطر المرتبطة بنشر أنظمة القياس الحيوي على الحق في خصوصية البيانات الشخصية؟

ما مدى كفاية التدابير التي تَضُمُّهَا «قانون الذكاء الاصطناعي» في الاتحاد الأوروبي لحماية الحق في خصوصية البيانات الشخصية في سياق أنظمة التعرف الحيوي؟

ما هي المقترحات الممكنة لتطوير الإطار التشريعي لتحقيق الموازنة بين تشجيع الابتكار المرتبط بتطور تقنيات القياس الحيوي وحماية الحق في خصوصية البيانات الشخصية؟

منهج البحث:

اعتمد البحث على المنهج الوصفي الذي يقوم على أساس بيان المقصود ببيانات القياس الحيوي، الصور التي تتخذها تلك البيانات، والتعرف على أنظمة القياس الحيوي مبينا طريقة عملها، تطبيقاتها المتعددة، واعتمد أيضا على المنهج التحليلي القائم على تحليل المخاطر المرتبطة بنشر تكنولوجيا القياس الحيوي على

الحقوق الفردية وخاصة الحق في خصوصية البيانات الشخصية، وعرض الأساليب والأليات التي وفرها «قانون الذكاء الاصطناعي» في الاتحاد الأوروبي لتلافي المخاطر المرتبطة بنشر أنظمة القياس الحيوي على الحق في خصوصية البيانات الشخصية وتحليلها؛ بغية الوقوف على مدى كفاية التدابير التي تضمنها هذا القانون لحماية الحق في خصوصية البيانات الشخصية في سياق أنظمة التعرف الحيوي، وصولاً إلى تكوين نهج قانوني مكتمل يحقق التوازن بين تشجيع الابتكار المرتبط بتطور تقنيات القياس الحيوي وحماية الحق في خصوصية البيانات الشخصية

أهداف البحث:

يحاول البحث تحقيق هدف رئيسي يتمثل في دراسة مدى تعقيد حماية البيانات الشخصية في مواجهة التحديات والمخاطر المرتبطة بنشر تكنولوجيا القياس الحيوي على الحق في الخصوصية لبيان مدى كفاية التدابير التي تضمنها «قانون الذكاء الاصطناعي» في الاتحاد الأوروبي لحماية الحق في خصوصية البيانات الشخصية في سياق أنظمة التعرف الحيوي؛ ويندرج تحت هذا الهدف مجموعة من الأهداف الفرعية أبرزها:

- بيان المقصود ببيانات القياس الحيوي، الصور التي تتخذها تلك البيانات.
- التعرف على أنظمة القياس الحيوي مبينا طريقة عملها، تطبيقاتها المتعددة.
- رصد التحديات والمخاطر المرتبطة بنشر تكنولوجيا القياس الحيوي على الحقوق الفردية وخاصة الحق في خصوصية البيانات الشخصية.
- الأساليب والأليات التي وفرها «قانون الذكاء الاصطناعي» في الاتحاد الأوروبي لتلافي المخاطر المرتبطة بنشر أنظمة القياس الحيوي على الحق في خصوصية البيانات الشخصية.
- تحليل مدى كفاية التدابير التي تضمنها «قانون الذكاء الاصطناعي» في الاتحاد الأوروبي لحماية الحق في خصوصية البيانات الشخصية في سياق أنظمة التعرف الحيوي.
- اقتراح توصيات لتطوير الإطار التشريعي لتحقيق الموازنة بين تشجيع الابتكار المرتبط بتطور تقنيات القياس الحيوي وحماية الحق في خصوصية البيانات الشخصية.

ولتحقيق هذا الهدف قُسمَت الدراسةُ إلى أربعة مباحث:

- **المبحث الأول:** ماهية بيانات وأنظمة القياس الحيوي.
- **المبحث الثاني:** المخاطر الناشئة عن بنية وأساليب استخدام أنظمة القياس الحيوي.
- **المبحث الثالث:** التنظيم القانوني لأنظمة التعرف الحيوي في قانون الذكاء الاصطناعي «AI Act».
- **المبحث الرابع:** مدى كفاية قانون الذكاء الاصطناعي في الحد من المخاطر الناشئة عن استخدام أنظمة التعرف الحيوي.

المبحث الأول

ماهية بيانات وأنظمة القياس الحيوي

تقوم أنظمة التعرف الحيوي على جمع ومعالجة بيانات القياس الحيوي؛ الأمر الذي يقتضي التعرف على المقصود بتلك البيانات، وبيان صورها المتعددة، كما يتطلب أيضاً التعرف على أنظمة التعرف الحيوي، وبيان طريقة عملها، وتطبيقاتها الشائعة؛

وهو ما سوف نتعرض له على النحو الآتي:

المطلب الأول

ماهية بيانات القياس الحيوي وصورها

تُعرف بيانات القياس الحيوي على أنها: «أي موقف يسمح بالتفاعل بين الإنسان والآلة باستخدام إحدى تقنيات القياس الحيوي»^(٤).

وعرّفتها اللائحة العامة لحماية البيانات (GDPR)^(٥) - في المادة ٤ - منها - على أنها: «البيانات الشخصية الناتجة عن معالجة فنية مُحددة تتعلق بالخصائص الجسدية أو الفسيولوجية أو السلوكية للشخص الطبيعي، والتي تسمح أو تؤكد الهوية الفريدة لهذا الشخص الطبيعي؛ مثل صور الوجه، أو بيانات المسح الضوئي للأصابع»^(٦)، كما أكد قانون الذكاء الاصطناعي على ذات المفهوم^(٧).

وتهدف أنظمة القياسات الحيوية إلى (التعريف: تحديد هوية الشخص، المصادقة: التحقق من هوية الشخص، التصنيف: تصنيف الأفراد على أساس خصائصهم، التعرف على المشاعر: تحديد الحالة العاطفية للشخص)^(٨)؛ عن طريق استخدام بعض الخصائص؛ منها البيولوجية (كبصمات الأصابع، صور الوجه، وصورة قرنية العين)، ومنها السلوكية (كنمط توقيع الشخص في الكتابة)

(4) Gary Roethenbaugh, cited in A Cavoukian, Privacy and Biometrics (Information and Privacy Commissioner, Ontario 1999) 11 <http://www.ipc.on.ca/images/Resources/pri-biom.pdf> accessed 31 May 2025.

(5) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) <https://eur-lex.europa.eu/eli/reg/2016/679/oj> accessed 31 May 2025.

(6) GDPR, Art 4 “... (14) ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;...”

(7) AI Act, Art 3 (34).

(8) AI Act, Recital 14.

صُور بعض تقنيّات القياس الحيوي:

ميّز بعضُ الباحثين في بعض الأحيان بين الخصائص البيولوجيّة والفسيولوجيّة^(١)؛ وكذلك الخصائص السلوكيّة، ونظرًا لعموميّة الخصائص «البيولوجيّة»، وكونها أكثرَ شمولًا من الخصائص «الفسيولوجيّة»؛ فقد اقترح آخرون استخدام مصطلح الخصائص «البيولوجيّة»؛ لشموله كلّ خصائص جسم الإنسان^(٢).

ويُشترطُ في تلك الخصائص أن تكون قابلةً للكشف، والاستخراج من مُميّزات قابلة للمقارنة والتعرّف عليها آليًا، كما ينبغي أيضًا أن تتباين تلك المُميّزات بين الأفراد المختلفين بشكلٍ كبير؛ وهو ما يُعبّر عنه بـ «variation interclass»؛ ومن أبرز الأمثلة على ذلك «قرحيّة العين»، وفي الوقت ذاته الذي تُشير فيه إلى حدٍّ أدنى من الاختلاف عند قياس المُميّزات الخاصّة بذات الشخص، وهو ما يُعبّر عنه بـ «variation class-intra»؛ ومن الأمثلة على ذلك «صُور الوجه»^(٣)؛ حيث تختلف صُورة الوجه للشخص ذاته بشكلٍ ضئيلٍ في الظروف المختلفة؛ كالتقدم في العمر مثلاً.

وبالنسبة لتحليل الجُمض النووي البشري «DNA»، فنظرًا لصعوبة القيام به آليًا؛ لم يُعدّ من قبيل تقنيّات القياس الحيوي؛ وذلك برغم أهميّته في تحديد هُوية الفرد بشكلٍ فريدٍ؛ تمامًا كتقنيّات القياس الحيوي الأخرى^(٤).

(1) The term 'physiological' refers to physiology ('fysiologie'/'physiologie'). Physiology is a branch of biology and deals with the functions and vital processes of living organisms (or their parts (e.g., cells and molecules) and organs), including the human body. Biology (from the Greek words 'βίος' (life) and 'λογος' (reason) is the science of life, living organisms, including their (physical) structure, function, growth, origin, evolution and processes.

يُشير مصطلح «فسيولوجيّة» إلى علم وظائف الأعضاء؛ وهو فرعٌ من علم الأحياء؛ يتناول وظائف الكائنات الحيّة (أو أجزائها) مثل الخلايا والجزيئات، الأعضاء) وعملياتها الحيويّة، بما في ذلك جسم الإنسان. علم الأحياء (المشتق من الكلمتين اليونانيتين «βίος» (حياة) و«λογος» (سبب) هو علم الحياة، والكائنات الحيّة؛ بما في ذلك بُنيّتها (المادّيّة)، ووظيفتها، ونموها، وأصلها، وتطورها، وعملياتها.

W Boron and E Boulpaep, Medical Physiology (Elsevier 2008).

(2) Article 29 Data Protection Working Party, Working Document on Biometrics, WP 80, 1 August 2003, 11 ('WP 29 Working Document on Biometrics 2003 (WP80)'); Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies, WP 193, 27 April 2012.

(3) Joseph Pato and Lynette Millett (eds), *Biometric Recognition: Challenges and Opportunities* (National Research Council, September 2010) 3 ('NRC, Biometric Recognition, 2010').

(4) Organization for Economic Co-operation and Development, *Biometric-based Technologies* (OECD, DSTI/ICCP/REG(2003)2/FINAL, 30 June 2004, cancelling and replacing the same document of 28 April 2004) 11 ('OECD, Biometric-based technologies, 2004').

أولاً: صور الوجه «Image Facial»:

يُمكن التقاط صور الوجه لأي فرد بسهولة تامة؛ سواء أكان ذلك بمعرفة صاحبها أم لا؛ وذلك بغرض التعرف على هويته عن طريق أنظمة التعرف على الوجه «system recognition facial»، وتستخدم تلك التقنية جميع أنواع الصور؛ سواء أكانت ثنائية الأبعاد، أم ثلاثية الأبعاد، والتي تُنتجها جميع أنواع الكاميرات؛ كما تستخدم الأشعة تحت الحمراء في مسح صور الوجه.

وتقوم هذه التقنية على تحليل صور الوجه بطرق مختلفة؛ فقد يركز التحليل، على سبيل المثال، على السمات الهندسية للوجه، كما قد يعتمد أيضاً على المسافة النسبية بين نقاط معينة، وقد يُستخدَم في أخرى نسيج الجلد⁽¹³⁾، وفي هذا الشأن يُمكن التمييز بين نوعين من العمليات، الأولى: تحديد هوية الفرد، وتتم تلك العملية عن طريق مقارنة بيانات القياس الحيوي للفرد (التي يتم الحصول عليها وقت الفحص)، مع نماذج القياس الحيوي المخزنة في قاعدة بيانات؛ أما الثانية: التحقق من هوية الفرد؛ وتتم تلك العملية عن طريق هوية الشخص «وقت الفحص»، مع نموذج قياس حيوي «واحد فقط» مُخزن داخل أحد الأجهزة

وتتمثل الفكرة الرئيسة لتلك التقنية في جمع صور الأشخاص بواسطة تقنية «CCTV»، ومقارنتها ببيانات القياس الحيوي المخزنة في شكل صور عالية الوضوح؛ وذلك لتحديد هوية الفرد أو التحقق منها، ويستخدم في ذلك تقنيات معينة تتضمن مسح الوجه بالأشعة تحت الحمراء ثنائية الأبعاد وثلاثية الأبعاد⁽¹⁴⁾.

وتم استخدام تلك التقنية في مجال أمن الطيران؛ حيث تم تطوير تلك الخاصية من أجل تحديد الأشخاص الخطرين من خلال مقارنة بيانات القياس الحيوي «البيومترية (الحية) المدخلة»- مع صورة وجه الراكب الملتقطة من خلال تقنية «CCTV مع قواعد بيانات المجرمين أو المشتبه بهم المعروفين

وتطبيقاً لذلك؛ فقد أصدرت بعض الدول كالولايات المتحدة الأمريكية، وبعض دول الاتحاد الأوروبي جوازات سفر تدعم تقنيات القياس الحيوي؛ والتي سمحت بمقارنة البيانات المُدخلة من صورة الوجه؛ لتسهيل التحكم الآلي في الحدود⁽¹⁵⁾.

(13) Organization for Economic Co-operation and Development, Biometric-based Technologies (OECD, DSTI/ICCP/REG(2003)2/FINAL, 30 June 2004, cancelling and replacing the same document of 28 April 2004) 26 (*OECD, Biometric-based technologies, 2004*), OP. Cit.

(14) Liu50، مرجع سابق، ص 50.

(15) Commission Decision of 28 June 2006 laying down the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States.

وتجدر الإشارة إلى وجود ما يُسمّى بالقياسات الحيوية «المرنة» (soft biometrics)، والتي تستخدم سماتٍ فرديةً شائعةً بين عددٍ مُعيّن من البشر؛ بحيث لا تسمح بالتعرّف على الفرد أو تحديد هويّته؛ وإنما تستهدف فصل القياسات الحيوية بواسطة الجهاز المستخدم من أجل تحديد ما إذا كانت الخصائص الخاصّة بشخص معيّن تنتمي إلى مجموعة ذات خصائص محددة سلفاً من أجل اتخاذ إجراء مُعيّن، وتُستخدَم تلك التقنية في أغراض مُعيّنة أمنية، وتجارية؛ حيث تُمكنُ- مثلاً- الشركات العاملة في مجال الإعلان من تحديد الفئات المستهدفة من خلال عرض إعلانات مختلفة؛ اعتماداً على عُمر الفرد أو جنسه، وتتميّز تلك التقنية بمراعاة الضوابط الخاصة بحماية البيانات الشخصية؛ لأن البيانات التي تتّهم معالجتها لا تتعلّق بشخص طبيعي «مُحدّد»، أو «يمكن تحديده»؛ ومن ثمّ، فلا تُعدّ من قبيل البيانات الشخصية⁽¹⁶⁾.

ثانياً: بصمة الإصبع «Fingerprint»:

تحتوي الأصابع على نُشوءات ومنخفضات؛ وتُشكّل تلك النتوءات أنماطاً على شكل أقواس ومنحنيات وحلقات، وتُعتبر تلك الأنماط الثلاثة أساساً لأنظمة التصنيف التي طوّرها «Vucetich»، و«Henry»

بينما تعتمد بعض الأنظمة الأخرى على أنماط تُسمّى «s'delta and cores»، وتقوم تلك الطريقة على وجود نُقطة مُحدّدة تُسمّى «Minutiae»؛ والتي تعني «انقطاع تدفق النتوءات الموجودة في إصبع الشخص»، أو «نمط تشعب تلك النتوءات»

ويتمّ الحصول على تلك البصمات بواسطة أجهزة الاستشعار، والتي تحتاج بالطبع إلى موافقة الشخص صاحب تلك البصمة، كما يمكن أيضاً الحصول على البصمات الكامنة «fingerprints latent»؛ كتلك الموجودة في مسرح الجريمة

كما يُستَترَطُ لاستخدام تلك التقنية أن تكون صورة البصمة على درجة عالية من الوضوح؛ لذا فقد استخدم بعض مُطوّري أنظمة القياس الحيوي تقنيات حديثة؛ لزيادة وضوح الصورة، وتقليل ما يُمكن أن يعترّيها من شوائب

(16) Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies* (WP 193, 27 April 2012).

ثالثاً: قُرْحية العين «Iris»:

تحوي قُرْحية العين قدرًا كبيرًا من معلومات القياس الحيوي؛ وذلك عن طريق الحلقة الملونة حول حدقة العين؛ حيث يعمل جهاز الاستشعار على التقاط البنية التفصيلية الفريدة لتلك الحلقة من خلال الشخص «موضوع البيانات» مباشرة؛ وذلك عن طريق إضاءة العين بواسطة الأشعة تحت الحمراء، كما يعمل جهاز الاستشعار على اكتشاف المميزات الأخرى؛ كالجفون، أو الرموش، أو الانعكاس الناتج عن النظارات؛ وذلك لاستبعادها أثناء الالتقاط، وقبل ترميز تلك البيانات في شكل « قالب - Template »

كما تجدر الإشارة إلى أن التقنيات الحديثة تسمح بالتقاط المعلومات حول قُرْحية العين عن بُعد، ودون علم شخص صاحبها^(١٤).

رابعاً: هندسة اليد «Geometry Hand»:

تُعَدُّ تقنية «هندسة اليد» من أولى تقنيات القياس الحيوي التي سمحت بمقارنة المعلومات المستخلصة منها «اليَا» بالمعلومات الموجودة في مرجع مخزن^(١٥)؛ وتعتمد تلك التقنية شكل وحجم اليد؛ حيث يتم قياس راحة اليد، طولاً، وعرضاً، وسُمك الإصبع، وكذلك المواقع النسبية لتلك المميزات؛ وذلك من الناحية الهندسية فقط، مع استبعاد جميع العوامل الأخرى التي لا صلة لها بتلك التقنية كتفاصيل سطح اليد، وكذلك بصمات الأصابع، والتئوءات، والندوب، أو الألوان

وعلى خلاف بصمة اليد؛ فإن تفرّد القياسات الهندسية لليد في البشر تبقى محدودة، كما لا تُعْطِي نتائج جيدة في التطبيق على نطاق واسع؛ لذا فقد كان استخدام تلك التقنية في أغراض التحقق من هوية الأفراد محدوداً، واقتصر استخدامها على نطاق ضيق^(١٦).

وإضافة إلى ما تقدّم؛ فإن أنظمة القياس الحيوي التي تعتمد على تلك التقنية تفتقر إلى الدقة؛ لأن القياسات الهندسية لليد عرضة للتغيير الناجم عن فقدان أحد الأصابع، أو تشوه اليد، وكذا الإصابة ببعض الأمراض «كالتهاب المفاصل»؛ كما قد يحدث ذلك التغيير نتيجة للتقدم في العمر.

(14) J R Matey et al, 'Iris on the Move: Acquisition of Images for Iris Recognition in Less Constrained Environments' (2006) Proceedings of the IEEE 1936-1947 <http://ieeexplore.ieee.org/Xplore/login.jsp?url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F5%2F4052463%2F04052478.pdf&authDecision=203> ('Matey et al., Iris on the Move, 2006').

(18) المرجع السابق، ص 38.

(19) A K Jain, A Ross and S Pankanti, 'A Prototype Hand Geometry-based Verification System', in Proceedings of the Second International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA) (Washington DC, USA, 1999); Joint Research Centre (JRC), Biometrics at the Frontiers (2005) 62.

خامساً: بصمة راحة اليد «Print Palm»:

تُعتبرُ بصمة راحة اليد من تقنيات القياس الحيوي الفريدة التي تستخدمها بعض أنظمة القياس الحيوي؛ حيث تحتوي راحة اليد على نتوءات ومنخفضات؛ كما هو الحال في بصمة اليد، كما تحتوي كذلك على خطوط وتجاويف^(١٧).

كما تتعيّن التفرقة بين تلك التقنية، وبين سابقتها، وقد تعتمد بعض الأنظمة التي تستخدم تقنية راحة اليد، على الخصائص الهندسية لليد في حساباتها لتحديد هويّة أحد الأفراد.

سادساً: الصوت «Voice»:

يُعدّ صوت الشخص من الخصائص التي تُستخدَم في بعض أنظمة القياس الحيوي، والتي تعتمد على ميزات الشخص البيولوجية والسلوكية، وتقوم تلك التقنية على تخزين صوت الشخص في خطابٍ مُحدّد، والمقارنة بينه وبين صوت الشخص ذاته عندما يتحدث مرّةً أخرى

ويُستخدَم الصوت في التّعرّف، أو التّحقّق من هويّة صاحبه، كما يتمّ استخدامه على نطاقٍ واسعٍ في تطبيقات الطبّ الشرعي^(١٨).

سابعاً: شبكية العين «Retina»:

تُعتبر شبكية العين بما تُسكّله الأوعية الدموية داخلها من أنماط، من المميزات الفريدة التي تُستخدَم في تحديد، أو التّحقّق من هويّة أحد الأشخاص، وتعتمد تلك التقنية على تحليل المسح الشبكي لطبقة الأوعية الدموية الموجودة في الجزء الخلفي من مقبلة العين، وتُستخدَم في ذلك المسح «الأشعة تحت الحمراء»، أو الأشعة القريبة من الأشعة تحت الحمراء.

(20) National Science and Technology Council (NSTC), Palm Print Recognition (2006) 10 <http://www.biometrics.gov/documents/palmprintrec.pdf>.

(21) Speech Technology Center, Voice Biometrics: Exciting Capabilities of a New Biometric Modality (presentation at Rise and Hide Conference, Brussels, 9–10 December 2010) slides 2, 4 and 14 http://www.riseproject.eu/_fileupload/RISE%20Conference/Presentations/Alexey%20Khitrov.pdf accessed 31 May 2025.

ونتيجةً للدقة العالية التي تتميز بها تلك التقنية؛ فقد تمَّ اعتمادها في المجالات العسكرية؛ إلا أنه- ومع ذلك- فقد انخفضت شعبيتها، بالمقارنة بتقنيات القياس الحيوي الأخرى؛ نظرًا لأنها تحتاج درجة كبيرة من الجهد والتعاون من قبل الشخص «موضوع البيانات»^(١٩)؛ لذا فقد اقتصر استخدامها على تقييد الدخول لبعض الأماكن الحكومية أو العسكرية؛ مثل الولوج إلى مواقع الأسلحة النووية

ثامناً: أنماط الأوردة «Patterns Vein»:

تُعَدُّ أنماط الأوردة من أحدث التقنيات التي تمَّ استخدامها في أنظمة القياس الحيوي؛ حيث تُشكِّل بنية الأوردة التي تُوجَد تحت الجلد في بعض أجزاء من جسم الإنسان أنماطاً فريدةً وواضحة ومستمرة يُمكنُ من خلالها تحديد، أو التحقق من هوية الشخص؛ مثال ذلك، بنية الأوعية الدموية الكائنة في راحة اليد، الأصابع، ظهر اليد، أو المعصم، وتُستخدَم تلك التقنية بعض الخصائص؛ مثل نقاط تفرُّع الأوعية الدموية، سُمْك تلك الأوعية، ويتم التقاط تلك الأنماط بواسطة كاميرا عالية الدقة تُستخدم الأشعة تحت الحمراء، أو الأشعة القريبة من الأشعة تحت الحمراء، ثم يتمُّ ضغط تلك الأنماط، وتحويلها إلى أرقام لتتمَّ المقارنة بينها بواسطة تقنية مطابقة الأنماط «technique matching- pattern»^(٢٠).

وتنتج أنظمة القياس الحيوي التي تُستخدم تلك التقنية نتائج فائقة الدقة، كما سمح التطوُّر التكنولوجي الحديث بالتقاط تلك الصور- دون علم الشخص «موضوع البيانات»- كالصور التي يتمُّ التقاطها في وقتٍ قصير أثناء الحركة^(٢١).

تاسعاً: الخصائص السلوكية «Characteristics Biometric Behavioral»:

تُستخدَم الخصائص السلوكية في أنظمة القياس الحيوي، وتمتدُّ تلك الخصائص لتشمل نمط وخصائص الكتابة أو التوقيع الذي يَعْتَمِدُ بالضرورة على سلوك الشخص الذي يُعْتَبَرُ فريداً أو على الأقل متميزاً، ونظرًا للطبيعة النشطة للشخص «موضوع تلك البيانات»؛ فقد سُمِّيت طُرُقُ القياس الحيوي التي تستندُ إلى تلك الخصائص بـ «طرق القياس الحيوي النشطة»، وقد سمَّاها آخرون بتلك التسمية؛ لضرورة تعاون الشخص الذي تستندُ إليه تلك الخصائص، حتى تتمكَّن أجهزة القياس الحيوي من تخزين بعض خصائصه السلوكية.

(22) Andy Ashbourn, *Social Implications of Wide Scale Implementation of Biometrics* (2005) 6.

(23) National Science and Technology Council (NSTC), *Privacy & Biometrics* (2006) 20, Op. Cit.

(24) Y Zhou and A Kumar, 'Contactless Palm Vein Identification Using Multiple Representations' (presentation and paper, IEEE Fourth International Conference on Biometrics: Theory, Applications and Systems (BTAS 2010), Washington DC, 27-29 September 2010) 6.

وبالنسبة لخصائص الكتابة؛ فالطريقة التي يستخدمها أحدهم للكتابة، أو الضغط على لوحة المفاتيح؛ مثل إيقاع الكتابة، وتكرار الأخطاء يُمثّل نمطاً فريداً يُمكن تحليله بواسطة البرامج؛ حيث يكشف ذلك التحليل عن أنماط الكتابة، وينتج مقياساً رقمياً يُمكن من خلاله مقارنته بالأنماط المسجلة مُسبقاً، وتُستخدَم تلك التقنية في مجال كلمات المرور؛ للتحقق مما إذا كانت صادرةً عن الشخص ذاته من عدمه

ومن الخصائص السلوكيّة التي تُستخدَم كذلك في أنظمة القياس الحيوي «النمط الحركي للتوقيع»؛ وهو ما يُعرَف بـ «**characteristics signature dynamic**»^(٢٢)، وتقوم تلك التقنية على تحليل التوقيع الذي يُكتَب بواسطة «القلم الذكي»، أو على لوح إلكتروني بواسطة بعض البرمجيات؛ (ويتضمّن ذلك التحليل بعض العناصر؛ منها: «السرعة، الضغط، اتجاه التوقيع»)، وتُستخدَم تلك التقنية للتحقق من هوية أحد الأشخاص في بعض المجالات القانونية والمعاملات التجارية؛ إلا أنه لا ينبغي الاعتماد عليها وحدها؛ نظراً لتغيرها بمرور الوقت، وتأثرها بالحالة البدنية والعاطفية للشخص^(٢٣).

عاشراً: خصائص القياس الحيوي «المُستحدثة»:

يُفترض أن يكون لكل شخصٍ مشيئةً مُميّزة «**Gait**»، وقد استُخدِمت تلك الخاصيّة المُعقّدة في بعض أنظمة القياس الحيوي، كما يجري تطويرها لكي تُستخدَم في التعرف على هوية الأشخاص عن بُعدٍ

ومن بين خصائص القياس الحيوي المُستحدثة: الرائحة «**odor**»؛ فكل شخصٍ رائحة مُميّزة، التي يُمكن استخدامها في أنظمة القياس الحيوي عن طريق تحليل المواد الكيميائية التي تتكوّن منها، كما تمّ استخدام بعض الخصائص الأخرى؛ كالشكل الخارجي للأذن، وشكل قناة الأذن، والتي لا تزال قيد التطوير^(٢٤).

(25) M Gasson, M Meints and K Warwick (eds), *D.3.2: A Study on PKI and Biometrics* (FIDIS, Frankfurt, July 2005) 82–86

(26) European Commission, *Convergence: Creating the Future* Commission. President Jacques Santer Announces 200,000 ECU European IT Prize Winners (25 November 1997) <http://cordis.europa.eu/esprit/src/eitcp4en.htm> accessed 31 May 2025.

(27) P Tuyls, E Verbitskiy, T Ignatenko, D Schobben and T Akkermans, *Privacy Protected Biometric Templates: Acoustic Ear Identification* (paper submitted at SPIE 2004) <http://www.sps.ele.tue.nl/members/T.Ignatenko/papers/SPIE2004.pdf> accessed 31 May 2025.

وبالإضافة إلى ما تقدّم؛ فقد استخدم بعض أنظمة القياس الحيوي أنماط المُخّ، وإيقاع القلب؛ بهدف التعرف على الهوية؛ حيث يُستخدَم تخطيط القلب «ECGs» لقياس إيقاع القلب، بينما يُستخدَم الرسم الكهربائي للمخ «EEGs»؛ لتسجيل أنشطة المُخّ الإلكترونية، والتي تُوفّر مميزات فريدة يتباين فيها البشر^(٢٥).

ومن المعلوم أنّ التعبير عن المشاعر يتمّ بواسطة تقاسيم الوجه؛ لذا فقد كانت موضوعاً للتحليل لاستخدامها في أنظمة القياس الحيوي، وتعمل تلك التقنية على تسجيل المشاعر الإنسانية مثل «الاهتمام، الإحباط، الغضب، أو الحزن...»

وتُستخدَم تقنية ترميز الوجه «coding face» في مجموعة واسعة من التطبيقات؛ منها التطبيقات المُستخدَمة في صناعة الترفيه، وكذلك لفهم والتأثير على السلوك الشرائي للأشخاص في المجال التجاري

(28) HUMABIO Project, Human Monitoring and Authentication Using Biodynamic Indicators and Behavioral Analysis (EU Sixth Framework Programme, 2006–2008) http://cordis.europa.eu/fetch?CALL-ER=IST_UNIFIEDSRCH&ACTION=D&DOC=6&CAT=PROJ&QUERY=011e5a6ef5cd:570d:08b-193fe&RCN=78373 accessed 31 May 2025.

المطلب الثاني

ماهية أنظمة القياس الحيوي وتطبيقاتها

تُعَرَّف أنظمة القياس الحيوي - في قانون الذكاء الاصطناعي - على أنها: «أنظمة آلية تَجْمَع وتُخزّن وتُعَالِج البيانات الحيويّة التي تسمح بتحديد هويّة الأشخاص أو التحقق منها؛ استناداً إلى خصائصهم البيولوجيّة أو السلوكيّة؛ مثل بصمات الأصابع، أو صور الوجه، أو قزحيّة العين...»^(٢٦).

أولاً: طريقة عمل أنظمة التّعرف الحيوي:

تتضمّن عمليّة نشر تقنيّات القياس الحيوي عادة عدة خطوات تتمثل في:

أ- جمع البيانات الأولى «التسجيل»: ويتمّ في هذه المرحلة استخدام أجهزة الاستشعار لالتقاط بيانات القياس الحيوي الخام في شكل تناظريّ أو رقمي؛ وهي البيانات التي تُمثّل الخصائص الحيويّة الفريدة للفرد؛ مثل هندسة الوجه، أو بصمة الإصبع، أو تسجيل الصوت.

ب- إنشاء المفتاح أو القالب «استخراج الميزة»: هي عمليّة استخدام التكنولوجيا لتحليل العيّنة الحيويّة لاستخراج مزايا فريدة ومميّزة، كما يتمّ تحويل هذه المزايا إلى تمثيل خوارزمي أو قالب خاصّ بهذا الفرد.

والقالب هو ملف ذو مساحة أصغر كثيراً من البيانات الأولى «الخام»، يُستخدَم لأغراض التخزين والمطابقة؛ فالنظام الحيوي لا يُخزّن صورة لبصمة الإصبع أو الوجه، بل يُخزّن تمثيلاً رياضياً لها.

ج- المطابقة أو التسجيل: هي عمليّة مقارنة عيّنة حيويّة جديدة بالمفتاح أو القالب الذي تمّ إنشاؤه في قاعدة البيانات

د- تخزين العيّات الحيويّة المُجمّعة (إدارة البيانات) وذلك في بعض الأنظمة⁽²⁷⁾:

نظراً لاستخدام الأنظمة الحيويّة المتعدّدة لخوارزميات وتنسيقات بيانات مختلفة؛ لذا يلجأ مطوِّرو هذه التكنولوجيا إلى مُنظّمات المعايير؛ لضمان الاتّساق على مستوى الصناعة فيما يتعلّق بـ(المصطلحات: يمكن أن يكون للمصطلحات التقنيّة تفسيرات مُتعدّدة، مقاييس الجودة والأداء: تضمن قيام الأنظمة الحيويّة بتلبية مستويات جودة معيّنة، معالجة مخاوف الأمن والخصوصيّة: تحديد أفضل الممارسات لتخزين البيانات، والتشفير، والتحكم في الوصول)، ويُمكّن الإشارة في

(29) AI Act, Art 3 (35).

(٣٠) تتضمّن بعض أنظمة القياس الحيوي خطوة أخرى تتمثّل في «التخلص من القوالب» في حالة عدم الحاجة إليها.

هذا الصدد إلى معايير المفردات الحيوية لمنظمة المعايير الدولية (ISO) ^(٢٨).

وتتعلق القدرات الأساسية للتقنيات الحيوية بالتعرّف أو التحقق ^(٢٩) أو التصنيف:

التعرّف: تتم مقارنة عينة حيوية تمّ التقاطها بجميع العينات المخزنة في قاعدة البيانات؛ بهدف تحديد هوية فردٍ من قاعدة بيانات كبيرة؛ ومن الأمثلة على ذلك: الأنظمة الوطنية لتحديد الهوية، تحديد هوية المشتبه بهم

التحقق: تتم مقارنة عينة حيوية تمّ التقاطها بعينة واحدة (أو مجموعة صغيرة) من العينات المرتبطة بالهوية المعلنة؛ بهدف تأكيد هوية شخص يدّعي أنه شخصٌ مُعيّن؛ ومن الأمثلة على ذلك: (التحكم في الوصول: فتح فُفل هاتفٍ ذكي، الدخول إلى مبنى مُعيّن / المعاملات المالية: المصادقة على المدفوعات عبر الإنترنت)

التصنيف: يتم تحليل البيانات الحيوية لاستنتاج سماتٍ؛ مثل الجنس، أو العمر، أو وجود أجزاءٍ مُعيّنة من الجسم بهدف تصنيف الأفراد إلى مجموعاتٍ فرعيةٍ؛ بناءً على خصائصهم الحيوية؛ ومن الأمثلة على ذلك: التحقق من العمر فيما يتعلق بالخدمات المقدّمة عبر الإنترنت، تحديد الجنس اللازم للتحليل الديموغرافي، اكتشاف الحيوية لتجنب الاحتيال

ومن ثمّ؛ فإن نوع النظام الحيوي يُؤثّر بشكلٍ مباشرٍ على مُتطلبات حوكمة البيانات؛ فعلى سبيل المثال يتطلب نظام التعرّف الحيوي قاعدة بياناتٍ كبيرة من العينات الحيوية على نحوٍ يستوجب تنفيذ تدابيرٍ أمنيةٍ أكثر صرامةً لحماية الخصوصية؛ نتيجةً لجمع البيانات على نطاقٍ واسع، وإمكانية إساءة استخدامها

ثانياً: التطبيقات الشائعة لأنظمة التعرّف الحيوي:

يرجع تاريخ التطبيقات الأولية لأنظمة التعرّف الحيوي؛ (مثل أنظمة بصمات الأصابع) إلى أواخر القرن التاسع عشر ^(٣٠)؛ إلا أنه، ونظراً للإمكانات الكبيرة التي وفّرها التقدّم التكنولوجي؛ مثل الاستخدام الآلي، وسهولة الوصول إلى بيانات القياس الحيوي؛ خاصّةً عند دمجها مع تقنياتٍ أخرى؛ مثل الذكاء الاصطناعي؛

(30) International Organization for Standardization (ISO), ISO/IEC 2382-37:2022 – Information Technology – Vocabulary – Part 37: Biometrics (2022–23) <https://www.iso.org/standard/73514.html> accessed 31 May 2025.

(٣٢) تُعرّف المنظمة الدولية للمعايير «التعرّف الحيوي» بأنه: «التعرّف الآلي على الأفراد؛ بناءً على خصائصهم البيولوجية والسلوكية»، ويعتبر التعرّف الحيوي مصطلحاً شاملاً لكلٍ من التعريف الحيوي والتحقق الحيوي.

(33) Office of Biometric Identity Management, Biometrics (US Department of Homeland Security) <https://www.dhs.gov/biometrics> accessed 31 May 2025.

الأمر الذي أدّى للوصول إلى ابتكاراتٍ على قَدْرٍ كبيرٍ من الأهميّة في مجال الأمن وإمكانية الوصول، ونتيجةً لذلك؛ فقد استُخدِمت أنظمة التعرف الحيوي على نطاقٍ واسعٍ في القطاعين العام والخاص

القطاع العام:

تستخدم السلطات العامة أنظمة القياس الحيوي كوسيلة للتحقق من صحة الوثائق وهوية حاملها (وثائق الهوية)، ولأغراض «تحديد الهوية – إنشاء الهوية – فحوصات التسجيل المزدوج»؛ ومن ذلك على سبيل المثال (أنظمة اللجوء، أنظمة تحديد الهوية على المستوى الوطني)، وقد تم إنشاء العديد من الأنظمة على مستوى الاتحاد الأوروبي⁽³¹⁾.

وفي مجال تنفيذ القانون: استخدمت الشرطة في لندن تقنية التعرف على الوجه على نطاقٍ واسعٍ، وتُستخدَم حاليًا من قبل الشرطة في ولاية سكسونيا الشرقية الألمانية، واستخدمتها كذلك شرطة برلين في نطاق جرائم العصابات العابرة للحدود⁽³²⁾.

وفي مجال الأمن: استُخدِمت هذه التكنولوجيا بغرض التحكم في الدخول إلى بعض الأماكن التي تتطلب أمنًا مُشدّدًا كخزائن البنوك، كما اكتسبت أهمية خاصة لدى الحكومات؛ حيث لعبت دورًا مهمًا في عديدٍ من المجالات؛ مثل الأمن، الهجرة، وتأمين الحدود⁽³³⁾.

وفي المجال الصحي: استُخدِمت أنظمة التعرف على الوجه بشكلٍ واسعٍ في:

أ- التشخيص الطبي لتحديد الحالات الوراثية النادرة؛ بناءً على سمات الوجه⁽³⁴⁾، أمراض التوحد، ومتلازمة كوشينغ “Cushing”، ومتلازمة كورنيليا دي لانج “Cornelia de Lange”⁽³⁵⁾.

(34) Graham Greenleaf, ‘India’s National ID System: Danger Grows in a Privacy Vacuum’ (2010) *Computer Law & Security Review* 26(5), 479–491.

(35) M Borak, ‘Police in Germany Using Live Facial Recognition’ (8 May 2024) Biometric Update <https://www.biometricupdate.com/202405/police-in-germany-using-live-facial-recognition> accessed 31 May 2025.

(33) Regulation (EC) No 2252/2004 of 13 December 2004 on Standards for Security Features and Biometrics in Passports and Travel Documents Issued by Member States [2004] OJ L385/1.

(36) Dian Hong and others, ‘Genetic Syndromes Screening by Facial Recognition Technology: VGG-16 Screening Model Construction and Evaluation’ (2021) 16 *Orphanet Journal of Rare Diseases* 1; ‘Use of Facial Recognition Technology for Medical Purposes: Balancing Privacy with Innovation’ (2016) 43(4) *Pepperdine Law Review* 1017, 1022.

(37) RP Kosilek and others, ‘Automatic Face Classification of Cushing’s Syndrome in Women – A Novel Screening Approach’ (2013) 121(9) *Experimental and Clinical Endocrinology & Diabetes* 561; L Basel-Vanagaite and others, ‘Recognition of the Cornelia de Lange Syndrome Phenotype with Facial Dysmorphology Novel Analysis’ (2016) 89(5) *Clinical Genetics* 557.

ب- التَّعَرُّفُ على المريض بِمُجَرَّدِ دخوله المستشفى، وإعادة توجيهه على الفور إلى الخدمة؛ حيث يتمُّ تحديد الموعد الطبي، باستخدام رسالة نصيَّة قصيرة، أو رسالة داخل التَّطبيقات لتوفير الوقت والجهد⁽³⁶⁾.

ج- تسهيل عمليَّات القبول للمرضى فاقدِي الوعي، أو المرضى الذين يُواجهون صعوباتٍ في التواصل؛ (مثل الأطفال، أو المرضى المسنين، أو المرضى ذوي الإعاقة العقليَّة)⁽³⁷⁾.

د- تتبَّع البيانات الصحيَّة ذات الأهميَّة -؛ مثل الحساسِيَّة، وفصيلة الدم، والإجراءات الصحيَّة السابقة - بسهولة من خلال ربط وجه المريض على الفور بسجله الصحي الإلكتروني⁽³⁸⁾.

هـ- التَّحكُّم في إمكانيَّة الوصول إلى أماكن محدَّدة في المنشأة الصحيَّة للمرضى وأقاربهم وكذلك العاملين في مجال الصحي⁽³⁹⁾.

(36) Kanubhai K Patel, Jignesh J Patoliya and Miral M Desai, 'IoT Based Smart Health Monitoring System with Patient Identification Using Face Recognition' in *Proceedings of the International Conference on Innovative Computing & Communication (ICICC)*, 2021).

(37) Byoungjun Jeon and others, 'A Facial Recognition Mobile App for Patient Safety and Biometric Identification: Design, Development, and Validation' (2019) 7(4) *JMIR mHealth and uHealth* 1.

(38) Barak Bassman and others, 'Facing Up to Tough Issues: Health Care Compliance Concerns with Facial Recognition Technology' (*JDSupra*, 12 May 2021) <https://www.jdsupra.com/legalnews/facing-up-to-tough-issues-health-care-9118586/> accessed 31 May 2025.

(39) Daniel Florez Mendez and others, 'Facial Recognition System for Security Access Control' (2021) 11842 *Proceedings of SPIE: Applications of Digital Image Processing XLIV* 1184217.

القطاع الخاص:

تُستخدَمُ أنظِمةُ القياس الحيوي بشكل متزايد في القطاع الخاص في العديد من المجالات؛ منها:

- ١- تعزيز أمن الوصول إلى منطقة محددة؛ حيث يقوم أصحاب العمل بتثبيت تطبيقات قياسات حيوية لتأمين، ومراقبة دخول موظفيهم إلى مقر العمل
- ٢- يستخدم أصحاب المحلات أو منظمو الأحداث العامة أنظِمةَ قياس حيوية للتحكُّم في الدخول أو للمراقبة؛ بهدف تعزيز السلامة العامة؛ مثل: مباريات كرة القدم.
- ٣- تُستخدَمُ أيضًا لأغراض إدارية؛ مثل التحكُّم في توقيت الحضور والانصراف للعمال، وتسجيل وجبات الطعام للطلاب في المدارس
- ٤- التحكُّم في إمكانية الوصول بالنسبة للأندية والمنشآت الرياضية الخاصة. وقد استُخدِمت كذلك في مجالات الحياة اليومية؛ مثل فتح الهواتف الذكية، أو الوصول إلى الحسابات الشخصية.

المبحث الثاني

المخاطر الناشئة عن بنية وأساليب استخدام أنظمة القياس الحيوي

تُصنّف بيانات القياس الحيوي في اللائحة العامة لحماية البيانات «GDPR» على أنها: «فئة خاصّة من فئات البيانات الشخصية»؛ ويرجع ذلك لارتباطها جوهرياً بالهوية الجسدية للفرد، مما يجعلها حساسة بشكل كبير؛ حيث تُؤدّي إلى إضعاف الأشخاص الذين تُشير إليهم هذه البيانات – ويُقصد بالضعف: «احتمال التعرّض للأذى الجسدي أو المعنوي»^(٤٠) – ويزداد هذا الضعف عندما يكون التعرّض للأذى أكثر احتمالاً؛ الأمر الذي قد يحدث نتيجةً لعدّة أسباب

وبشكلٍ عام، يُمكن أن تنشأ المخاطر على أصحاب البيانات من بنية وأساليب استخدام نظام القياس الحيوي، أو من أي هجوم على النظام الحيوي يُمكن أن يكون له عواقب وخيمة على الشخص صاحب البيانات، بالإضافة إلى ذلك يُمكن أن تتبّع هذه المخاطر من تشريعات ولوائح حماية البيانات ذاتها في الحالات التي تسمّح فيها بمعالجة بيانات القياس الحيوي

المطلب الأول

المخاطر المتعلّقة بالتنظيم القانوني للبيانات الشخصية

اغْتُبِرَت بيانات القياس الحيوي – كما سبق أن ذكرنا- ضمن «فئات البيانات الخاصة»، ومن ثمّ فإنها تخضع لقواعد أكثر صرامة؛ فقد حظرت اللائحة العامة لحماية البيانات – في المادة (٩) منها^(٤١) – معالجة هذه البيانات من حيث الأصل.

ومع ذلك؛ فإن التنظيم الصارم لللائحة العامة لحماية البيانات لا ينطبق على حالات معيّنة؛ فوفقاً للمادة 2(2)؛ فإنّ اللائحة العامة لحماية البيانات “لا تنطبق على معالجة البيانات الشخصية: (أ) في سياق نشاط يقع خارج نطاق قانون الاتحاد؛ (ب) من قبل الدول الأعضاء عند القيام بأنشطة تقع ضمن

(40) Vocabulary.com, ‘Vulnerability’ <https://www.vocabulary.com/dictionary/vulnerability> accessed 31 May 2025.

(41) Art. 9 “ 1- Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.....”

نطاق الفصل 2، من الباب الخامس من معاهدة الاتحاد الأوروبي TEU؛ (ج) من قبل شخص طبيعي في سياق نشاطٍ شخصي أو منزلي بحث؛ (د) من جانب السلطات المختصة لأغراض منع الجرائم الجنائية، أو التحقيق فيها، أو اكتشافها، أو مقاضاة مرتكبيها، أو تنفيذ العقوبات الجنائية؛ بما في ذلك الحماية من التهديدات التي يتعرّض لها الأمن العام^(٢٢)، بالإضافة إلى أن الحظر الوارد في المادة (٩) من اللائحة العامة لحماية البيانات – سالف الذكر – لجمع هذه البيانات ومعالجتها ليس حظرًا مطلقًا، وإنما تردُّ عليه عدة استثناءات نصّت عليها ذات المادة؛ من بينها:

أ- موافقة الشخص المعنيّ بالبيانات على معالجة البيانات الشخصية الحساسة الخاصة به لغرض معيّن؛ إلا أنه استثنى من ذلك الحالات التي ينصّ قانون الاتحاد، أو قانون إحدى الدول الأعضاء على عدم الاعتداد برضاء الشخص المعنيّ بالبيانات لرفع ذلك الحظر^(٢٣).

ب- أن تكون معالجة هذه البيانات ضرورية لتنفيذ التزامات وممارسة الحقوق الخاصة بمراقب البيانات، أو الشخص المعنيّ بالبيانات في مجال العمل والضمان الاجتماعي، والحماية الاجتماعية بالقدر الذي يسمح به قانون الاتحاد الأوروبي، أو قانون إحدى الدول الأعضاء، أو اتفاق جماعي ووفقًا لقانون الدولة ذات العضوية؛ والذي يشترط أن ينصّ على ضمانات مناسبة لحماية حقوق الشخص ومصالحه «موضوع البيانات»⁽⁴³⁾.

ومن ثم يُمكنُ تطبيق قواعد أكثر مرونة، وهو ما يوفر الحماية الكافية للأفراد فيما يتعلق ببياناتهم الشخصية.

(42) Art. 9 “ 2- Paragraph 1 shall not apply if one of the following applies:

1- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.....”

(43) Art. 9 “ 2- Paragraph 1 shall not apply if one of the following applies: 2- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.....”

أولاً: التّحديات المتعلّقة بالأساس القانوني لمعالجة البيانات:

تستلزم أي معالجة للبيانات الشخصية وجود مبرر قانوني؛ وهو ما يُعرّف باسم «الأساس القانوني لمعالجة البيانات»، ونظراً لحساسية بيانات القياس الحيوي؛ فإنّ معالجة هذا النوع من البيانات تتطلب وجود سببين قانونيين: أحدهما للبيانات الشخصية العامة (المادة ٦ من اللائحة العامة لحماية البيانات)، والآخر للبيانات الحساسة (المادة ٩ من اللائحة العامة لحماية البيانات)

وينظر العديد من مراقبي البيانات إلى «موافقة صاحب البيانات»؛ باعتبارها الأساس القانوني الأيسر للمضي قدماً في معالجة البيانات؛ إلا أنه – وفقاً لنصّي المادتين 6 (1) (أ)، 9 (2) (أ) من اللائحة العامة لحماية البيانات – تُعدّ الموافقة معياراً يصعبُ الامتثال إليه؛ ويرجع ذلك إلى عدّة أسباب (٤٤)؛ تتمثل في:

أولاً: يجب أن تكون المعلومات المُقدّمة للشخص موضوع البيانات واضحةً وموجزةً ومناسبةً لمستوى فهم الفرد المستهدف، وفيما يتعلّق بتقنيّات القياس الحيوي؛ يجب أن تتضمّن المعلومات: مواقع تنفيذ التقنيّة، هويّة مُستخدمي البيانات، مدة الاحتفاظ بالبيانات، وطريقة الاحتفاظ بها، إجراءات ممارسة الحقوق الممنوحة بموجب اللائحة العامة لحماية البيانات (٤٥).

كما يجب أن تكون الموافقة صريحةً؛ وهو ما يعني ضرورة اتّخاذ موقف إيجابي؛ فلا يُمكنُ أن تُستنبط هذه الموافقة ضمناً من سلوك مُعيّن (٤٦)؛ لذا فإنّ مجرد دخول شخص لمنشأة مع علمه بتشغيل تقنيّة تعمل على جمع البيانات الحيوية، لا يمكن اعتباره موافقةً صريحةً على جمع ومعالجة بياناته؛ ومن ثمّ يصبح الحصول على موافقة كلّ مَنْ يدخل إلى تلك المنشآت المزودة مستحيلاً من الناحية العمليّة

ثانياً: عبء إثبات الموافقة: تقع مسئولية إثبات حصول الموافقة على عاتق «جهات التحكّم» في البيانات – وفقاً لنصّ المادة ٧ (١) من اللائحة العامة لحماية البيانات – وفي ظل صعوبة إثبات الموافقة الشفويّة؛ يُعدّ الحصول على موافقة كتابيّة من كل زائر أمراً في غاية الصعوبة كذلك (٤٧).

(44) European Data Protection Board, Guidelines 05/2020 on Consent under Regulation 2016/679 (May 2020) 7–32 https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf accessed 31 May 2025.

(45) European Data Protection Board, Guidelines 3/2019 on Processing of Personal Data Through Video Devices (January 2020) 5–23 https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices.pdf accessed 31 May 2025.

(46) GDPR, OP. Cit, Recital 32.

(47) Opinion 3/2012, OP. Cit.

والفرض الأكثر صعوبة يتعلّق بتشغيل تقنية قياس حيوي لغرض التحكم في الدخول إلى بعض المرافق؛ حيث يجب الحصول على موافقة مجموعة كبيرة غير معروفة من الأفراد، التي لا تكون هويتهم – في معظم الحالات – معلومة مسبقاً؛ مما يجعل الامتثال لأحكام اللائحة العامة لحماية البيانات أمراً مستحيلاً من الناحية العملية

كما يجب أن تكون الموافقة – نُزولاً على أحكام اللائحة العامة لحماية البيانات- طوعية؛ ولا تكون الموافقة كذلك إلا إذا كانت لدى صاحب البيانات القدرة على عدم تقديمها دون التعرّض لتبعاتٍ تُؤثّر سلباً عليه، وفي هذا السياق اعتُبرت سلطات حماية البيانات أن الموظفين لا يمتلكون الحرية الكاملة في رفض الموافقة على معالجة بياناتهم؛ نتيجةً لتبعيّتهم للمرفق الذين يعملون به⁽⁴⁸⁾؛ ففي المرافق الصحية مثلاً قررت بعض سلطات حماية البيانات أن موافقة المريض لم تكن حرة؛ نتيجةً لخشية الحرمان من الرعاية الصحية إذا اعترض على جمع ومعالجة بياناته، وكما ذكر مكتب مفوض المعلومات (ICO) – سلطة حماية البيانات بالملكة المتحدة- «إذا لم تتمكّن من تقديم خيار حقيقي؛ فإنّ الموافقة تكون غير مناسبة» وإذا استمرت الرغبة في معالجة البيانات دون الحصول على موافقة؛ فإن الإصرار على طلبها يُعدّ أمراً مضللاً⁽⁴⁹⁾.

ونتيجةً لاستحالة الحصول على موافقة الجميع؛ يجب تنفيذ التقنيات التي تعمل على جمع ومعالجة بيانات القياس الحيوي بطريقة تسمح بمعالجة بيانات من يوافق على استخدامها دون الآخرين عن طريق ترتيب مسار بديل لدخول وخروج المبنى دون مراقبة، وإذا تحقق ذلك؛ فإنّ الهدف الأساسي من تنفيذ التقنية – التحكم في الدخول والخروج من المبنى- سيكون معرضاً للخطر؛ مما يجعل التكنولوجيا عديمة الفائدة

وبناءً على ما سبق، يُمكن القول إنّ هناك عدة تحديات قانونية وعملية تتعلّق بمحاولة تلبية متطلبات الموافقة – كأساس قانوني لمعالجة البيانات- على النحو المنصوص عليه في المادتين 6 (1) (أ)، 9 (2) (أ) من اللائحة العامة لحماية

البيانات؛ ومن ثمّ يجب استكشاف أسس قانونية أخرى لمعالجة البيانات؛ مثل: حماية المصالح الحيوية للشخص موضوع البيانات "المادة 9(2) (ج)"، المصلحة المشروعة «المادة 6 (1) (ب)».

(48) European Data Protection Board, Guidelines 3/2019, OP. Cit.

(49) Information Commissioner's Office, 'Consent' (ICO, n.d.) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/> accessed 31 May 2025.

ثانياً: التّحديات المتعلّقة بمبدأ تقليل البيانات:

تلتزم وحدات التحكّم في البيانات التي تقوم بجمع البيانات الشخصية ومعالجتها بأن تقتصر على البيانات الملائمة، الضرورية، المتعلّقة بالغرض الذي تمّ جمعها من أجله⁽⁵⁰⁾؛ وهو ما يُطلَق عليه «مبدأ تقليل البيانات - The data-minimisation principle» - الذي تناولته المادة (5) من اللائحة العامة لحماية البيانات - فيجب على الجهات المُنوطة بها جمع ومعالجة البيانات الشخصية أن تدرس بعناية الغرض من معالجة البيانات الخاصة بها، وألا تجمع إلا الحد الأدنى من البيانات الشخصية المطلوبة لتحقيق هذا الغرض

ويهدف هذا المبدأ إلى ضمان عدم قيام المؤسسات بجمع، أو الاحتفاظ ببيانات غير ضرورية؛ بما يُعزّز من خصوصية البيانات، ويُقلّل من المخاطر المتعلّقة باختراق البيانات

إلا أن استخدام أنظمة القياس الحيوي في الأماكن العامة أدّى إلى انتهاك حقوق الأفراد في حماية بياناتهم الشخصية، على نحو تعارض مع المبادئ العامة الحاكمة لمعالجة البيانات الشخصية؛ ومن بين تلك المبادئ «مبدأ تقليل البيانات»؛ فقد جرى انتهاك هذا المبدأ في الممارسة العملية؛ الأمر الذي دفع السلطات العامة في العديد من الدول إلى التّدخل لحماية المصلحة العامة؛ فقد عاقبت هيئة حماية البيانات الإيطالية أداة «التعرّف على الوجه - FRT» الخاصة بشركة Clearview AI؛ لانتهاك المبادئ الخاصة بالشفافية، والحد من الغرض، تقليل البيانات من خلال جمع بيانات القياس الحيوي، وبيانات تحديد الموقع الجغرافي دون أساس قانوني سليم⁽⁵¹⁾، وبرغم مواجهة غرامات تتجاوز قيمتها ٢٠ مليون يورو من سلطات حماية البيانات المختلفة في الاتحاد الأوروبي⁽⁵²⁾

(50) Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Modernised Convention 108, 2018), art 5(4) (c); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), art 5(1)(c).

(51) European Data Protection Board, 'Facial Recognition: Italian SA Fines Clearview AI EUR 20 Million' (2022) https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en accessed 31 May 2025.

(52) NOYB – European Center for Digital Rights, 'Clearview AI Data Use Deemed Illegal in Austria, However No Fine Issued' (2023) <https://noyb.eu/en/clearview-ai-data-use-deemed-illegal-austria-however-no-fine-issued> accessed 31 May 2025.

تواصل شركة Clearview AI، والشركات الأخرى تطوير خوارزميات تعمل على استخدام بيانات غير ضرورية «مُفرطة»

إن مبدأ تقليل البيانات لا يتعلّق بحماية الأفراد فقط؛ وإنما بحماية الجمهور بشكل عام⁽⁵³⁾؛ فالنطاق الواسع لأنشطة معالجة البيانات التي تقوم بها الهيئات القائمة على تنفيذ القانون – على سبيل المثال- دون وجود قواعد واضحة قد يُسبّب مخاوف تتعلّق بالمراقبة المستمرة؛ حيث تعمل هذه المراقبة الشاملة على تقويض استقلالية الأفراد بشكل كبير؛ مما يجبرهم على الامتنثال للسلوكيات المتوقعة في الأماكن العامة⁽⁵⁴⁾ – يُقصدُ بها المساحات التي يمكن لجمهور الناس الوصول إليها؛ سواء كانت مملوكة ملكية عامة أو خاصة⁽⁵⁵⁾، والتي يُشار إليها غالبًا باسم «البيئات غير الخاضعة للرقابة»⁽⁵⁶⁾؛ فاستخدام كاميرات المراقبة المزودة بتقنيات القياس الحيوي؛ يعني أن الأفراد الذين يمرّون بها يصبحون بالضرورة موضوعًا للمراقبة دون مبرر؛ ممّا يؤدي إلى خلق «بيئات خاضعة للرقابة»؛ حيث يشعر الأفراد أنهم مُجبرون على الامتنثال للمعايير والتوقعات المجتمعية؛ مما يحدّ من حريتهم وتعبيرهم عن أنفسهم⁽⁵⁷⁾.

(53) European Union Agency for Fundamental Rights, *Handbook on European Data Protection Law: 2018 Edition* (FRA, 2018) https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf accessed 31 May 2025.

(54) Clive Norris, 'From Personal to Digital: CCTV, the Panopticon, and the Technological Mediation of Suspicion and Social Control' in David Lyon (ed), *Surveillance as Social Sorting* (Routledge 2002) 249–281 <https://doi.org/10.4324/9780203994887> accessed 31 May 2025.

(55) لأغراض تطبيق هذه اللّائحة، يشير مفهوم «المساحة المتاحة للجمهور» إلى أي مساحة ماديّة يمكن الوصول إليها من قبل عددٍ غير محدد من الأشخاص الطبيعيين؛ سواء كانت هذه المساحة المعنيّة مملوكة ملكية خاصة أو عامة، وبغض النظر عن النشاط الذي يُمكن استخدام المساحة من أجله؛ مثل التجارة على سبيل المثال: (المحلات التجارية والمطاعم والمقاهي)؛ للخدمات: على سبيل المثال (البنوك والأنشطة المهنية والضيافة)؛ للرياضة؛ على سبيل المثال: (المسابح والصالات الرياضية والملاعب)؛ للنقل، على سبيل المثال (محطات الحافلات والمترو والسكك الحديدية والمطارات ووسائل النقل)؛ للترفيه، على سبيل المثال: (دور السينما والمسارح والمتاحف وقاعات الحفلات الموسيقية والمؤتمرات)؛ أو للترفيه أو غير ذلك، على سبيل المثال، الطرق العامة والساحات والحدائق والغابات والملاعب. ٢. تُصنّف المساحة أيضًا على أنها متاحة للجمهور إذا كان الوصول - بغض النظر عن السعة المحتملة أو القيود الأمنية - خاضعًا لشروط محددة مُسبقًا يُمكن استيفاؤها من قبل عدد غير محدد من الأشخاص؛ مثل شراء تذكرة، أو سند نقل، أو التسجيل المسبق، أو بلوغ سن معيّنة

AI Act, Op. Cit, Recital 19.

(56) Consultative Committee of the Convention 108, *Guidelines on Facial Recognition* (Guideline No T-PD(2020)03rev4, Council of Europe 2021) <https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html> accessed 31 May 2025.

(57) (i) David Lyon, 'Surveillance' (2022) 11(4) *Internet Policy Review* <https://doi.org/10.14763/2022.4.1673> accessed 31 May 2025.

ويرجع ذلك – بشكلٍ أساسي- إلى عدم إدراك الأفراد لمصير بياناتهم الملتقطة بواسطة هذه التقنيات، وعلى فرض تحقق هذا الإدراك؛ فقد يواجهون تحديات عديدة تتعلّق بممارستهم لحقوقهم؛ مثل الحق في المحو «النسيان»، الحق في تقييد معالجة البيانات المنصوص عليهما في المادتين (١٧، ١٨) على التوالي من اللائحة العامة لحماية البيانات؛ فحين تستهدف المراقبة مجموعة ما؛ فإنهم لا يملكون أيّ فرصة للإفلات من المراقبة، كما لا يمكنهم المطالبة بحقوقهم بشكلٍ جماعي؛ لأن اللائحة العامة لحماية البيانات لا تعترف بالحقوق الجماعية؛ ففي عام ٢٠١٨ استخدمت الشرطة البريطانية تقنية التعرف على الوجه «FRT» لمسح وجوه الأفراد المشاركين في احتجاج رسمي في مكان عام في المملكة المتحدة؛ الأمر الذي أدّى إلى إقامة دعوى قضائية لقيام الشرطة باستخدام هذه التقنية لمسح وجوه الجميع دون إبلاغهم بالتقييم الخوارزمي المُحتَمَل^(٥٨)، ونتيجةً لذلك؛ فقد شعر المُحتجّون بالقلق أثناء ممارستهم لحقوقهم في الاحتجاج؛ على الرغم من أن الهدف المُعلن من نشر هذه التقنية كان تعزيز الأمن العام؛ الأمر الذي كان له بالغ الأثر على الحقوق الأساسية للأفراد التي من بينها «الحق في الاحتجاج»

ثالثاً: التّحديات المتعلّقة بمبدأ تحديد الغرض:

نصّت اللائحة العامة لحماية البيانات «GDPR» على عدة حقوق لأصحاب البيانات؛ ترتب بعضها على المبادئ الأساسية لمعالجة البيانات الشخصية المنصوص عليها المادة (٥) من اللائحة؛ ومن هذه الحقوق: الحق في الحصول على المعلومات «Right to be informed» الذي تناولته اللائحة فيما نصّت عليه في المادة (١٣) منها^(٥٩)، فيجب إبلاغ أصحاب البيانات بدقّة بالغرض من جمع بيانات القياس الحيوي؛ حتى يتمكّنوا من فهم هذا الغرض بوضوح^(٦٠) ووفقاً للمجلس الأوروبي لحماية البيانات (EDPB)؛ يجب توفير المعلومات على

(58) *Bridges v Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin) <https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf> accessed 31 May 2025.

(59) Art.13 “ 1- Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller’s representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;.....”

(60) *Case C-275/06, Promusicae v Telefónica de España SAU* [2007] ECLI:EU:C:2007:454, Opinion of AG Kokott, para 53.

مرحلتين^(٦١): الأولى: اللقاء الأول بين صاحب البيانات ووحدة التحكم المسؤولة عن تنفيذ تقنية جمع بيانات القياس الحيوي، وتشمل هذه المرحلة أهم المعلومات، ويوصي المجلس الأوروبي لحماية البيانات باستخدام علامة تحذير في مكان يسهل رؤيته، مع رمز - المادة 12(7) من اللائحة العامة لحماية البيانات^(٦٢) - ولكنه يُقرّ بإمكانية تعديل تنسيق المعلومات حسب الموقع المُحدّد.

المرحلة الثانية: يجب أن تُتاح المرحلة الثانية من المعلومات التي يجب أن تُشير إليها المرحلة الأولى، في مكان يُمكن لأصحاب البيانات الوصول إليه بسهولة؛ على سبيل المثال: من خلال رمز الاستجابة السريعة (QR code)؛ أو رابط إنترنت، أو مكتب معلومات

وتتعلّق هذه المرحلة بمجموعة من الحقوق التي ترتبط بالغرض من جمع البيانات؛ فلا يجوز استخدام بيانات القياس الحيوي المُجمّعة لاحقاً لأغراض مختلفة؛ نظراً للقيود المفروضة بموجب المادة 5 (1)(ب) من اللائحة العامة لحماية البيانات^(٦٣)؛ والتي تهدف إلى منع خطر التداخل الوظيفي

إلا أنّ الطبيعة الخاصة لأنظمة الذكاء الاصطناعي شكّلت تحدياً كبيراً لمبدأ معالجة البيانات الشخصية لغرض محدد -- The principle of purpose limitation -- أحد المبادئ الأساسية لمعالجة البيانات الشخصية -؛ ففي الوقت الذي يتم فيه جمع بيانات القياس الحيوي في البداية لغرض مُحدّد يُمكن تدريب خوارزميات الذكاء الاصطناعي لتوليد مُخرجات تُحقّق أغراضاً أخرى؛ كاستخدام الكاميرات المُثبتة في مراكز التسوق لمراقبة الموظفين داخلها^(٦٤)، أو تحديد العرق، أو الروابط العائلية، وقد سمح هذا التحول الوظيفي - المعروف باسم التسلل الوظيفي function creep^(٦٥) - بمعالجة البيانات الشخصية بما يتجاوز الغرض الأساسي

(61) Guidelines 3/2019 (n 50) 26–27.

(62) Art.12 “...7- 1The information to be provided to data subjects pursuant to [Articles 13](#) and [14](#) may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. 2Where the icons are presented electronically they shall be machine-readable...”

(63) Art.5 “1- Personal data shall be: ... (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with [Article 89\(1\)](#), not be considered to be incompatible with the initial purposes (‘purpose limitation’);...”

(64) European Data Protection Board. (2020). Guidelines 3/2019 on processing of personal data through video devices, Op. cit.

(65) Koops B-J, ‘The Concept of Function Creep’ (2021) 13(1) *Law, Innovation and Technology* 29 <https://doi.org/10.1080/17579961.2021.1898299> accessed 31May 2025.

وإذا تعلّقت الأغراض اللاحقة بالبحث العلمي؛ فإنَّ الاستثناء المنصوص عليه في المادة (٨٩) من اللائحة العامة لحماية البيانات قد يَدْخُل حيز التطبيق، ومع ذلك يعتمدُ تحقيق هذا الاستثناء على عدّة متطلبات يصعبُ استيفاؤها عملياً (٦٦)؛ أهمها: وجوب إخفاء هوية البيانات، أو استخدامها كأسماء مُستعارة كلّما كان ذلك ممكناً

إلا أنَّ المشكلة الرئيسة تتعلّق بصعوبة إخفاء هوية بيانات القياس الحيوي؛ لأنها تشير إلى الخصائص الفريدة للشخص (٦٧)؛ فقد نصّت المادة ٤ (١٤) من اللائحة العامة لحماية البيانات على أنَّ بيانات القياس تُعدُّ بياناتٍ تعريفية فريدة تتعلّق بالخصائص الجسدية والفيسيولوجية أو السلوكية للشخص الطبيعي؛ مما يؤكد تلك الصعوبة، كما أنه، وبالإضافة إلى ذلك؛ فقد يُؤدّي تطوُّر تقنيّات الذكاء الاصطناعي إلى زيادة إمكانية إعادة تحديد هوية البيانات التي كانت – سابقاً – مجهولة المصدر

ومن ناحيةٍ أخرى، قد يَسْتَبْدُ التحول الوظيفي إلى موافقة صاحب البيانات كأساس قانوني للمعالجة – وفقاً لنص المادة ٦ (١) أ من اللائحة العامة لحماية البيانات – لكن هذه الموافقة قد تكونُ خادعة (٦٨)؛ خاصّةً عند استخدامها من قبل الهيئات القائمة على تنفيذ القانون؛ فعلى سبيل المثال لم تقتصر شركة Clear-view AI على معالجة البيانات الشخصية؛ بهدف تطوير النِّظام؛ وإنما قامت أيضاً بمعالجتها؛ تحقيقاً لهدف آخر؛ تمثّل في مراقبة الأفراد دون موافقتهم (٦٩)؛ وهو الأمر الذي يُؤكِّد وجودَ تفاوت في القوة بين السلطة والأفراد، يُصعِّبُ على الأفراد تقييم المخاطر، أو الحدّ من المراقبة؛ فعلى الرغم من الجهود التي تبذلها سلطات حماية البيانات – حيث عاقبت هيئة حماية البيانات السويدية الشرطة السويدية

(66) Alex van der Wolk and Morrison & Foerster, 'The (Im)Possibilities of Scientific Research Under the GDPR' (Cybersecurity Law Report, 2020) 3–4 <https://assets.contentstack.io/v3/assets/blt5775c-c69c999c255/bltbb2bb3df1bea55fe/200722-scientific-research-gdpr.pdf> accessed 31 May 2025.

(67) Banda J, 'Inherently Identifiable: Is It Possible to Anonymize Health and Genetic Data?' (IAPP, 13 November 2019) <https://iapp.org/news/a/inherently-identifiable-is-it-possible-to-anonymize-health-and-genetic-data> accessed 31 May 2025.

(٦٨) يُعَدُّ إرساء الموافقة كأساس قانوني لمعالجة البيانات في تقنيّات الذكاء الاصطناعي أمراً صعباً؛ لذا عادةً ما يُقدِّمُ مُحكمو البيانات تطبيقات موافقة لا تتوافق مع المبادئ الأساسية لمعالجة البيانات الشخصية.

Gültekin-Várkonyi G, 'Consent Mechanism in the Life with Social Robots' (2019) 31(1) *European Review of Public Law*.

(69) Rezende IN, 'Facial Recognition in Police Hands: Assessing the "Clearview Case" from a European Perspective' (2020) 11(3) *New Journal of European Criminal Law* 375 <https://doi.org/10.1177/2032284420948161> accessed 31 May 2025.

لاستخدام Clearview AI دون إشارة مُحدّدة إلى غرض المراقبة^(٧٠)؛ فإن التّطور التكنولوجي المتسارع يتجاوز القدرة على الاستجابة لهذا التحول الوظيفي، كما تُستخدم الجهات القائمة على تنفيذ القانون أدوات الذكاء الاصطناعي المتطوّرة - كجزء من مسؤولياتها المتعلّقة بالأمن العام -؛ مثل ChatGPT دون الحصول على موافقة الفرد، أو إعلام الجمهور^(٧١)، وبالإضافة إلى ما تقدّم؛ فقد تمّ تطوير تقنيّات أخرى؛ مثل «القياسات الحيويّة الناعمة - soft biometrics» للمساعدة في التنبؤ بالجرائم؛ بناءً على معلومة واحدة؛ مثل استنتاج عرق الشخص من خلال الملابس^(٧٢)، وقد أدت هذه التطوّرات إلى زيادة الشكوك حول استخدام تقنيّة التّعرّف على الوجه «FRT» في المراقبة على نطاق واسع في حين أن الغرض الرئيس من استخدامها يتمثّل في تعزيز الأمن العام.

رابعاً: التّحديات المتعلّقة بمبدأ دقّة البيانات:

تناولت المادة ٥ (د) من اللائحة العامّة لحماية البيانات مبدأً من أهم المبادئ الحاكمة لجمع البيانات ومعالجتها؛ وهو مبدأ «دقّة البيانات - The data accuracy principle»؛ حيث يلتزم مراقبو البيانات بالاقصّار على البيانات الشخصية الدقيقة المُحدّثة

وتبدو أهميّة هذا المبدأ - من الناحية العمليّة - في حماية حقوق الأفراد وحُرّيّاتهم؛ كحماية الأفراد من التوقيف والاستجواب المتكرّر من خلال الشرطة^(٧٣)، وحمايتهم كذلك من الاتّهام الخاطي؛ استناداً إلى بيانات غير دقيقة في قواعد البيانات الخاصّة بجهاز الشرطة^(٧٤).

(70) European Data Protection Board, *Swedish DPA: Police Unlawfully Used Facial Recognition App* (Press release, 2021) https://www.edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en accessed 31 May 2025.

(71) Europol, *ChatGPT: The Impact of Large Language Models on Law Enforcement (Tech Watch Flash)* (Europol Innovation Lab, 2023) <https://www.europol.europa.eu/publications-events/publications/chatgpt-impact-of-large-language-models-law-enforcement> accessed 31 May 2025.

(72) Wang Y-F, Chang EY and Cheng KP, 'A Video Analysis Framework for Soft Biometry Security Surveillance' in *Proceedings of the Third ACM International Workshop on Video Surveillance & Sensor Networks* (2005) 71 <https://doi.org/10.1145/1099396.1099412> accessed 31 May 2025.

(73) Dimitrov-Kazakov v Bulgaria (Application No 11379/03, ECtHR, 2018) <https://hudoc.echr.coe.int/eng?i=001-103258> accessed 31 May 2025.

(74) Hill K, 'Wrongfully Accused by an Algorithm' New York Times (24 June 2020) <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html> accessed 31 May 2025.

وتجدر الإشارة إلى أنه يجب التمييز بين نوعين من الدقة؛ حيث تنظر اللائحة العامة لحماية البيانات إلى مبدأ دقة البيانات؛ باعتباره مطلباً أساسياً لكي تكون البيانات صحيحةً وحديثةً وقابلةً للتصحيح، في حين يُشير مصطلح الدقة في إطار الذكاء الاصطناعي إلى مستوى الدقة الذي تخرجه الخوارزمية؛ سواء كانت رياضيةً أو إحصائيةً، فلم تشر اللائحة العامة لحماية البيانات إلى دقة البيانات الشخصية المباشرة فحسب؛ بل أشارت أيضاً إلى البيانات الشخصية التي تتم معالجتها بطريقة غير مباشرة، والتي يمكنها تحديد هوية الأفراد؛ مثل التصنيفات^(٧٥) أو الاستنتاجات؛ فيجب اعتبار التحليلات التي تُقدمها تقنيات القياس الحيوي بيانات شخصية؛ لاحتوائها على مخاطر تتعلق بمعالجة هذه البيانات؛ حيث تعمل على تصنيف الأشخاص بشكلٍ احتمالي وفقاً لدرجة خطورتهم

وفيما يتعلق بأنظمة القياس الحيوية، فبحسب طبيعتها وطريقة عملها، تُعدُّ عملية القياس مُعرضة للخطأ في كل مرحلة من المراحل؛ ابتداءً بمرحلة «التسجيل»، ومروراً بمرحلة «استخراج الميزة»، وانتهاءً بمرحلة «المقارنة»، ومن الجدير بالذكر أن الأخطاء تزداد في حالة استخدام وظيفة التعريف، مقارنةً بوظيفة التحقق

وتُقاس دقة النظام الحيوي بالمعدل الذي يقوم به هذا النظام بتسجيل البيانات الصحيحة للعينة المُجمعة مقابل سجلات القالب، مع الأخذ في الاعتبار التّطابق الخاطئ «الإيجابية الخاطئة - match False»، وعدم التّطابق الخاطئ «السلبية الكاذبة - match-non False»؛ فيحدث التّطابق الخاطئ عندما يتم مطابقة السمة الحيوية للفرد بشكلٍ غير صحيح مع سمةٍ من فرد آخر، في حين يحدث عدم التّطابق الخاطئ عندما يتم تحديد السمة الحيوية للفرد بشكلٍ غير صحيح على أنها لا تتطابق مع سمةٍ تمّ جمعها من ذات الفرد^(٧٦).

وتعتمد الدقة على عدّة عوامل؛ منها: نوع وجودة البيانات التي تمّ جمعها، عمر التكنولوجيا، عدد القوالب المُقدمة للمطابقة، وقد أشارت الاختبارات إلى ارتفاع

(75) Hacker P, 'AI Regulation in Europe: From the AI Act to Future Regulatory Challenges' (2023) <https://doi.org/10.48550/arXiv.2310.04072> accessed 31 May 2025.

(76) UK National Cyber Security Centre, Biometrics: Measuring Performance (2019) <https://www.ncsc.gov.uk/collection/biometrics/measuring-performance#:~:text=A%20false%20match%20occurs%20when,a%20characteristic%20from%20another%20individual> accessed 31 May 2025.

معدّلات الخطأ لدى الشباب^(٧٧)، حالة الشيخوخة، وخاصّةً بالنسبة للوجه^(٧٨)، والأشخاص من ذوي الاحتياجات الخاصّة^(٧٩)، وقد تتغيّر دقة بعض الخصائص الحيويّة بسبب عوامل؛ مثل الوقت أو المرض^(٨٠)، وبشكلٍ عام تزداد الدقة مع ازدياد عدد نقاط البيانات المتاحة.

ونتيجةً لمعدّلات الخطأ تلك؛ قد يتعرّض أصحاب البيانات إلى أضرارٍ مُتعدّدة تتباين في تأثيرها؛ فقد تكون بسيطةً؛ مثل تعرّض أصحاب البيانات المؤهلين للرفض بشكل خاطئ؛ مما يُؤثّر سلبيًا على حقوقهم الأخرى؛ كالحقّ في حرّية التنقل (الحق في السفر)، وقد أشارت مجموعة العمل المُشكّلة تطبيقًا لنص المادة ٢٩ إلى هذا الخطر؛ حيث ذكرت أنّ «التقنيّات المُطبّقة يجب أن تؤدي إلى مُعدّلات رفض زائفة منخفضة للغاية؛ نتيجةً للعواقب الوخيمة التي قد تمسّ حاملي الوثائق الشرعيين»، وقد تصل إلى التحيّز الشديد (التمييز)^(٨١)، وكذلك الاتّهام الخاطئ في مجال التحقيقات الجنائيّة، ومن ناحيةٍ أخرى، قد يترتّب على هذه المعدّلات زيادة احتماليّة تعرّض النظام للاحتيال؛ لذا يجب أن يكون أمن النظام موضع تساؤلٍ في حالة ارتفاع مُعدّلات الخطأ.

وفي الوقت الحالي، أضحت النّطبيقات الحديثة لتقنيّات القياسات الحيويّة أكثر دقةً من الإصدارات السابقة؛ خاصّةً عندما يتمّ دمج الخوارزميات مع الذكاء الاصطناعي؛ فقد نشر المعهد الوطني للمعايير والتكنولوجيا التابع لوزارة التجارة الأمريكيّة تقييمًا لتقنية التّعريف على الوجه المُستخدّمة في المطارات لأغراض «التحقّق»؛ حيث وجد أنّ الخوارزميات يُمكنها تنفيذ المهمّة باستخدام مسح واحد لوجه الراكب بدقة ٩٩,٥ ٪ أو أكثر. وخاصّةً عند احتواء قاعدة البيانات على صور مُتعدّدة للراكب^(٨٢)، ووجد المعهد أنّ دقّة الخوارزميات قد تحسّنت بشكل

(77) Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Kamerstuk 25 764, nr. 27b1 (2005) 83 <https://zoek.officielebekendmakingen.nl/kst-25764-27-b1.pdf> accessed 1 June 2025.

(78) U Park, Y Tong and AK Jain, 'Face Recognition with Temporal Invariance: A 3D Aging Model' (2010) IEEE Transactions on Pattern Analysis and Machine Intelligence 32(5), 947 <https://ieeexplore.ieee.org/document/5413023> accessed 1 June 2025.

(79) UK Passport Service, *Biometrics Enrolment Trial* (May 2005) 299.

(80) Esefan Ortiz, Kevin W Bowyer and Patrick J Flynn, 'A Linear Regression Analysis of the Effects of Age Related Pupil Dilation Change in Iris Biometrics' (2013) https://www3.nd.edu/~kwb/Ortiz_Bowyer_Flynn_BTAS_2013.pdf accessed 1 June 2025.

(٨١) يعني أي شكل من أشكال المعالجة الآلية للبيانات الشخصية التي تتضمن استخدام البيانات الشخصية لتقييم بعض الجوانب الشخصية المتعلقة بالشخص الطبيعي، وخاصّةً لتحليل أو التنبؤ بالجوانب المتعلقة بأداء الشخص في العمل، والوضع الاقتصادي والصحة، والتفضيلات الشخصية، والاهتمامات، والموثوقية، والسلوك، والموقع أو الحركات.

GDPR, OP. Cit, Art.4.

(82) National Institute of Standards and Technology (NIST), 'NIST Evaluates Face Recognition Software's Accuracy for Flight Boarding' (17 July 2021) <https://www.>

كبير بمرور الوقت، ومع ذلك، وحتى عندما تعمل تقنيات القياس الحيوي بدقة كبيرة، قد تحدث نتائج مُتحيزة، ومن ثمّ؛ يستلزم النشر المسؤول لهذه التقنيات حلولاً اجتماعية – تقنية «socio-technical»^(٨٣).

وللحدّ من المخاطر المتعلقة بمعدّلات الخطأ، يُمكن تطبيق أحد الحلول الآتية:

- تحديث قواعد بيانات المجال التشغيلي للتقنية المستخدمة، وتحسين دقة الخوارزمية^(٨٤)؛ إلا أنّ استخدام هذه الطريقة قد يترتب عليه تعزيز المراقبة في الأماكن العامة^(٨٥).
- استخدام قواعد البيانات المجمعّة مفتوحة المصدر التي تضمن إمكانية قياس مستويات الدقة^(٨٦)؛ إلا أنّ مُقدّمي الخدمات قد يُفضّلون استخدام قاعدة بيانات مُغلقة خاصّة بهم؛ ممّا يعوق تحقيق الشفافية؛ حيث لا يُمكن قياس مستويات الدقة بشكل مباشر^(٨٧)؛ كما قد تتأثّر موثوقية النظام إذا تضمّنت قاعدة البيانات المفتوحة صوراً مُزيّفة لا تُمثّل أفراداً حقيقيين.

nist.gov/news-events/news/2021/07/nist-evaluates-face-recognition-sofware-accuracy-flight-boarding accessed 1 June 2025.

(٨٣) يشير مصطلح «الاجتماعي التقني» إلى تحليل يأخذ في اعتباره كيفية التفاعل بين الجوانب الاجتماعية (المتعلّقة بالبشر والمنظمات)، والجوانب التقنية (المتعلّقة بالتكنولوجيا).

Oxford Reference, 'Socio-technical System' <https://www.oxfordreference.com/display/10.1093/oi/authority.20110803100515814> accessed 1 June 2025.

(84) AS Bergman and others, 'Representation in AI Evaluations' in Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency (2023) 519 <https://dl.acm.org/doi/fullHtml/10.1145/3593013.3594019> accessed 1 June 2025.

(85) VL Raposo, '(Do Not) Remember My Face: Uses of Facial Recognition Technology in Light of the General Data Protection Regulation' (2023) 32(1) Information & Communications Technology Law 45 <https://doi.org/10.1080/13600834.2022.2054076> accessed 1 June 2025.

(86) R Delikat, The Regulatory Gap Between the Law and the Use of Real-Time Facial Recognition Technology by Police in the European Union (Master's thesis, Tilburg University 2021) 61 <https://arno.uvt.nl/show.cgi?fid=155401> accessed 1 June 2025.

(87) I Fábíán and GG Gulyás, 'A Comparative Study on the Privacy Risks of Face Recognition Libraries' (2021) 25(2) Acta Cybernetica 233 <https://cyber.bibl.u-szeged.hu/index.php/actcybern/article/view/4198> accessed 1 June 2025.

لذا يغدو ضروريًا أن يكون لدى الجهات القائمة على إنفاذ القانون والجمهور كذلك القدرة على التساؤل عن مصدر البيانات، كما تُساعد المعايير الفنية^(٨٨) في تدريب الخوارزمية لتحسين دقة الأنظمة الحيوية، وتتكوّن هذه المعايير من عدّة عوامل منها: مواصفات الأجهزة، جودة الصُّور، زاوية التصوير، عمليّات إعداد البيانات؛ إلا أن هذه التفاصيل – في الكثير من الأحيان – لا يتمّ إعلانها للجمهور بشفافيّة

المطلب الثاني

المخاطر المتعلقة ببنية نظام القياس الحيوي

أولاً: صعوبة التسجيل:

تواجه العديد من الأنظمة الحيوية – وفقاً لما أشار إليه العديد من التقارير – صعوبةً في تسجيل الخصائص الحيوية لبعض الأفراد؛ حيث يُمكن لعوامل مثل العمل اليدوي (على سبيل المثال: اهتراء بصمات الأصابع؛ نتيجة الأعمال اليدوية الشاقة)، المناخ والظروف الجوية القاسية أن تُؤدّي إلى تدهور البيانات الحيوية؛ فالحصول على بيانات عالية الجودة يُعدّ أمراً بالغ الأهمية؛ حيث تُؤدّي البيانات ذات الجودة المنخفضة إلى زيادة مُعدّلات القبول والرفض الخاطئي^(٨٩).

وتكتسب هذه المخاطر أهميةً كبيرةً؛ حينما تكون البدائل المُتاحة للأفراد محدودة، كما هو الحال بالنسبة إلى أنظمة القياس الحيوي واسعة النطاق التي تُنظّمها الحكومة

وتجدرُ الإشارة إلى وجود عددٍ محدودٍ من الدراسات اختصّت بتحليل الصعوبات التي تُواجه عمليّة التسجيل؛ ومن بين هذه الدراسات تجربة خدمة جوازات السفر في المملكة المُتحدة عام ٢٠٠٥؛ والتي أشارت إلى أن حوالي ٩٠٪ من المُشاركين في التجربة نجحوا في التسجيل في خصائص القياسات الحيوية التي تمّ اختبارها؛ وهي (بصمة الإصبع، قُرْحِيّة العين، الوجه)^(٩٠).

وكشفت الدراسة عن تأثيراتٍ تمييزيّةٍ لدى مجموعات معيّنة؛ فبالرغم من أن غالبية المُشاركين من مجموعات العيّنة قد نجحوا في التسجيل في الخصائص التي تمّ اختبارها (بصمة الإصبع، قُرْحِيّة العين، الوجه)، إلا أن مُعدّلات النجاح كانت أقلّ بالنسبة للمُشاركين من ذوي الإعاقة (حوالي ٦٠٪)^(٩١).

(88) American Society for Testing and Materials, Standard Guide for Capturing Facial Images for Use with Facial Recognition Systems (ASTM International, 2023) Vol 14.02, No E3115-17 <https://doi.org/10.1520/E3115-17> accessed 1 June 2025.

(89) Erik Snijder, *Het biometrisch paspoort in Nederland: crash of zachte landing* (2010) 70–72.

(90) UK Passport Service, OP. Cit, p. 52.

(٩١) المرجع السابق، ص ٣٨.

فشل شخص واحد من بين كل ٢٠٠ شخص من ذوي الإعاقة في التسجيل في أي من الخصائص-

وقد أثارت مجموعة العمل المُشكَّلة وفقاً لنص المادة (٢٩)، وهيئة مراقبة حماية البيانات الأوروبية (EDPS) هذه المشاكل المتعلقة بالصعوبات التي تواجه عملية التسجيل، وفيما يتعلّق مثلاً بنظام معلومات التأشيرات: ذكر الجهاز الأوروبي للتأشيرات عام ٢٠٠٥ أنّ هناك ما يصل إلى ٥٪ من الأشخاص يُقدَّر أنهم غير قادرين على التسجيل؛ وهو ما أدى إلى نتيجة مؤدّاها «إذا توقَّع النظام حوالي ٢٠ مليون تأشيرة؛ فإن حوالي مليون شخص لن يكونوا قادرين على اتّباع إجراءات التسجيل العادية لهذا النظام»^(٩٢).

وتجدر الإشارة أيضاً إلى أن مُعدّل الفشل في التسجيل (FTE) – وفقاً للتعريف الوارد في مفردات ISO للقياسات الحيوية – لا يشمل عدد الأشخاص الذين لا يستطيعون إرسال الخاصية لعدم امتلاكهم إيّاها

ثانياً: اتخاذ قرارات ذات طابع تمييزي:

ذكرنا سابقاً أن بعض الفئات قد لا تمتلك الخصائص الحيوية المطلوبة، أو قد تكون هذه الخصائص أقلّ وضوحاً من المعدل الطبيعي؛ حيث تُواجه بعض الفئات كالأشخاص ذوي الإعاقة، والأشخاص في سنٍ محدّدة مخاطر تتعلّق بارتفاع معدلات الإخفاق

وبحسب بحثٍ منشورٍ صادرٍ عن المعهد الوطني للمعايير والتكنولوجيا، يُمكن لهذا التمييز أن يُضخّم ويديم الآثار السلبية على الأفراد والمؤسسات والمجتمع^(٩٣)؛ فقد كشفت ورقة بحثية مستقلة^(٩٤) نُشِرت عام ٢٠١٨ أنّ ثلاثة أنظمة تجارية رئيسية للتعرف على الوجه أظهرت مُعدّلات دقة أعلى للأفراد ذوي البشرة الفاتحة والذكور؛ وهو ما أشار إلى وجود تفاوتٍ في الأداء؛ بناءً على النوع، ولون البشرة

(92) EDPS (European Data Protection Supervisor), **Opinion on the Proposal for a Council Decision on the establishment, operation and use of the second-generation Schengen Information System (SIS II)** (2005) 19.

(93) Reva Schwartz and others, *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence* (NIST Special Publication 1270, 2022).

(94) Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (Conference on Fairness, Accountability, and Transparency, 2018) <https://www.media.mit.edu/publications/gender-shades-intersectional-accuracy-disparities-in-commercial-gender-classification/> accessed 1 June 2025.

ويُعرّف التمييز في الاتفاقيّة الأوروبيّة لحقوق الإنسان بأنه: «أيّ تمييز على أساس النوع، أو العرق، أو اللون، أو اللغة، أو الأصل القومي، أو الاجتماعي، أو الميلاد، أو أي سببٍ آخر»^(٩٥)، وقد ترك هذا الوصف المفتوح لمصطلح «التمييز»

حتمالاً يتعلّق باعتبار أي فقدان لأي سمة قياس حيوي (سليمة) سبباً للتمييز أيضاً، ولكي تنطبق أحكام عدم التمييز يكفي وجود: (١) اختلاف في المعاملة (٣) بين «أشخاص» أو «مجموعات أشخاص» في «مواقف مُماثلة»، أو «متشابهة إلى حدّ كبير» (٣) «دون مبرر موضوعي ومعقول»

ومن ثمّ، يقع على عاتق المدّعي عبء إثبات عدم وجود مبرر موضوعي معقول لتلك المعاملة المختلفة، وفي هذا الصدد؛ سوف تحتاج المحاكم إلى مراجعة ما إذا كان عدم قدرة أنظمة القياس الحيوي على التقاط البيانات، أو مقارنتها بسبب الجودة السيئة للبيانات، أو غياب أشخاص مُعيّنين يُعدّ مبرراً موضوعياً معقولاً لرفض الوصول أو فرض إجراءات تستغرق وقتاً طويلاً؛ (مثل المحاولات المُتعدّدة)، أو التسبب في نفقات؛ مثل (الاستئناف) لهؤلاء الأشخاص

ومنذ ذلك الحين؛ أظهر العديد من الدراسات أن الأنظمة الحيويّة يُمكن أن تنتج نتائج إيجابيّة أكثر لدى مجموعات النساء والأشخاص ذوي البشرة الداكنة والصغار والكبار؛ فقد أظهرت دراسة نشرها المعهد الوطني للمعايير والتكنولوجيا في ديسمبر ٢٠١٩؛ شملت (١٨٩) برنامجاً للتعرف على الوجه؛ أفادت بأنّ الخوارزميات المطوّرة في الولايات المتحدة كانت أكثر عرضة لإظهار نتائج إيجابيّة وسلبية خاطئة للأفراد ذوي البشرة الداكنة والآسيويين والأمريكيين الأصليين؛ مقارنةً بالأفراد ذوي البشرة الفاتحة^(٩٦)، كما خلصت دراسة أخرى أُجريت عام ٢٠٢٠ إلى أنّ أنظمة بصمات الأصابع عرضة للتحيز العمري؛ لأنها قد تختفي أو تصبح أقل وضوحاً بسبب العلاجات الطبيّة، أو التعرّض للمواد الكيميائيّة، أو العمل اليدوي^(٩٧).

ومن بين الآثار التمييزيّة الأخرى؛ أنّ الأفراد الذين يتمّ تسجيل بياناتهم الحيويّة، وتُخزّن في نظامٍ معين – على سبيل المثال (نظام التحكّم الحيوي في الوصول): الذي يثبت من خلاله دخول شخص ما مكاناً معيّن في توقيت محدد

(95) Article 14, Convention for the Protection of Human Rights and Fundamental Freedoms, Protocol No 12 (opened for signature 4 November 2000, entered into force 1 April 2005).

(96) National Institute of Standards and Technology (NIST), 'NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software' (19 December 2019) <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software>

(97) Andrea Rosales and Mireia Fernández-Ardèvol, 'Ageism in the Era of Digital Platforms' (2020) Convergence <https://journals.sagepub.com/doi/full/10.1177/1354856520930905>.

يعرضون أنفسهم لخطر المعاملة كمشتبه بهم في جريمة ما إذا تمّ إعادة استخدام هذه البيانات من قبل السلطات القائمة على تنفيذ القانون في سياق التحقيق في وقائع مُحَدَّدة تُشكِّل جريمة، وقد أشارت المحكمة الأوروبية لحقوق الإنسان إلى هذا الخطر في قضية S. AND MARPER v. THE UNITED KINGDOM^(٩٨).

وللحدّ من هذه المخاطر، هناك العديد من الطرق؛ أهمّها إعطاء الأولويّة للتنوّع والشمول في الفئات التي تُنشئ نماذج الذكاء الاصطناعي وتُراقبها، وكذلك فيما يتعلّق بالبيانات المُستخدمة لتدريبها^(٩٩)؛ إلا أنه ومع ذلك فقد يُعدّ تصنيف البيانات في حدّ ذاته تحدّيًا كبيرًا بسبب عدم الاتّفاق على التدابير القياسية، بالإضافة إلى قيام معظم قوانين حماية البيانات بتقييد جمع ومعالجة البيانات الشخصية الحسّاسة؛ (مثل: العمر، العرق، النوع)، وتستلزم للقيام بذلك وجود أسس قانونيّة مُحَدَّدة بالرغم من أهميّة هذا النوع من البيانات لأنظمة القياس الحيوي؛ حيث تُمكن المطوّر من قياس أداء النظام؛ مقارنةً بكل فئة أو مجموعة فرعيّة

علاوةً على ذلك، لا تتنظر قوانين حماية البيانات – في مُعظّم الأحوال – إلى «منع التحيز»؛ باعتباره غرضًا مشروعًا من أغراض معالجة البيانات الشخصية، وللتغلّب على هذه العقبة يجب الاعتراف بضرورة إيجاد مجموعاتٍ من البيانات المعتمَدة؛ بغرض تحقيق التنوع؛ حيث تتضمّن نقاط بيانات تمّ جمعها بشكل قانوني ليستخدّهما المطوّرون لتحقيق التنوع المادي بشكلٍ يمكن التحقّق منه

وتجدر الإشارة إلى أنّ العديد من أنظمة القياس الحيوي يتمّ نشرها عن طريق الأفراد الذي قد يرتكبون أخطاءً، أو يحملون تحيزًا، وبهدف معالجة هذه المخاطر، يجب على مطوّر أنظمة الذكاء الاصطناعي؛ بما في ذلك تقنيّات القياس الحيوي، تطبيق ما يُسمّيه باحثو المعهد الوطني للمعايير والتكنولوجيا (NIST) نهجًا «تقنيًا اجتماعيًا» يأخذ في اعتباره سياق التطبيق^(١٠٠)، الذي يتطلب - حال تنفيذه - مثلاً - من قبل الجهات القائمة على تنفيذ القانون أن تقوم هذه الجهات بالإفصاح عن استخدام تلك التقنيّات؛ بهدف مساعدتها في القيام بعملها، ومع ذلك؛ فلا تزال هناك حاجة إلى مزيدٍ من البحث لفهم سبب إظهار بعض الأنظمة الحيويّة لنتائج تمييزيّة، والكيفيّة التي يُمكن من خلالها الحدّ من هذه الأضرار.

(98) S and Marper v United Kingdom App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008) <https://hudoc.echr.coe.int/fre?i=001-90051>

(99) Ayanna Howard and Charles Isbell, 'Diversity in AI: The Invisible Men and Women' (21 September 2020) MIT Sloan Management Review <https://sloanreview.mit.edu/article/diversity-in-ai-the-invisible-men-and-women/>

(١٠٠) Schwartz et al، مرجع سابق، ص ٤٧.

ثالثاً: اتّخاذ قرارات بناء على المعالجة الآليّة:

تحظر المادة (٢٢) من اللائحة العامّة لحماية البيانات اتّخاذ القرارات؛ استناداً إلى المعالجة الآليّة وحدها؛ فيجب أن يكون لصاحب البيانات الحق في عدم الخضوع لقرار، أو إجراء يتضمّن تقييمًا لبعض الجوانب الشخصية الخاصّة به، استناداً إلى المعالجة الآليّة وحدها - دون أي تدخل بشري -؛ بما في ذلك «التميط Profiling» -، والتي قد تنتج آثاراً قانونيّة تُؤثّر بشكل كبير عليه (١٠١)، وتتخذ الجوانب الشخصية محلّ التقييم عدّة صور؛ منها: الأداء في العمل، الجدارة الائتمانيّة، ممارسات التوظيف الإلكتروني

وتقوم الأنظمة الحيويّة على عمليات آليّة تُعالج من خلالها خصائص معيّنة للشخص، الذي يُعامل لاحقاً على سند من هذه الخصائص؛ فحينما يكون الهدف من معالجة بيانات القياس الحيوي هو أتمّة إجراءات وقرارات معيّنة؛ مثل السماح بالدخول، أو رفض الدخول؛ فإن من شأن القرار الصادر في هذا الخصوص أن يحدث آثاراً قانونيّة، أو يُؤثّر بشكل كبير على الشخص صاحب البيانات، ومن ثمّ ينطبق عليه الحظر المنصوص عليه في المادة (٢٢) سالفه الذكر

إلا أن المادة (٢٢) ذاتها تضمّنت استثناءاتٍ لهذا الحظر نصّ عليها البند الثاني منها، وفيما يتعلّق بالفئات الخاصّة للبيانات «البيانات الحساسة»؛ ومن بينها بيانات القياس الحيوي؛ فإنّ الاستثناءات تقتصر على:

- الموافقة الصريحة لصاحب البيانات.
- المصلحة العامّة الجوهرية (تطبيقاً لنصّ المادة ٢٢ (٤) من اللائحة العامّة لحماية البيانات).

وفيما يتعلّق بالمصلحة العامّة الجوهرية؛ فلم تُحدّد اللائحة العامّة لحماية البيانات المقصود بها، إلا أنه يمكن القول إنها تشمل على الأرجح التهديدات المتعلّقة بالأمن أو الصّحة العامّة

وفي جميع الأحوال يجب اتّخاذ التدابير المناسبة لحماية حقوق وحريات صاحب البيانات ومصالحه المشروعة

وفي هذا السياق، أشارت مجموعة العمل المُشكّلة وفقاً لنصّ المادة (٢٩) بشكل متكرر إلى المادة (١٥) من التوجيه الأوروبي لعام ١٩٩٥ « Directive EC/٤٦/٩٥ - المُقابلة لنصّ المادة (٢٢) من اللائحة العامّة لحماية البيانات GDPR

(١٠١) GDPR, Recital 71.

وذكرت أنه في حالة إصدار نظام القياس الحيوي قرارًا خاطئًا بالرفض، فيجب إبلاغ الأشخاص بأسباب ووسائل تأكيد وجهة نظرهم^(١٠٢).

واحترامًا للحق الأساسي في احترام حقوق الدفاع^(١٠٣)، وكذلك حقوق كبار السن والأشخاص ذوي الاحتياجات الخاصة في التمتع بالحماية^(١٠٤)؛ يجب التأكيد على حق صاحب البيانات في الطعن على القرارات التي تتخذها تطبيقات القياسات الحيوية، والذي قد يتضمن: طلب التدخل البشري لمزيد من التدقيق، أو إجراء استئناف أكثر رسمية^(١٠٥).

رابعًا: الموثوقية والتوفر:

يجب على الجهات القائمة على تنفيذ تقنيات القياس الحيوي مراعاة العوامل التي تؤثر على توفر التكنولوجيا وموثوقية العينات لتحقيق الفائدة المرجوة من تطبيقات القياسات الحيوية؛ حيث تؤثر جودة العينات الحيوية بشكل كبير على دقة تحديد الهوية؛ فعلى سبيل المثال، قام نظام التعرف الآلي المتكامل على بصمات الأصابع «IAFIS» الذي طوره مكتب التحقيقات الفيدرالي الأمريكي «FBI» بمطابقة بصمات أحد المشتبه بهم بشكل خاطئ مع تلك التي عُثِرَ عليها في موقع هجوم إرهابي في مدريد عام ٢٠٠٤، وبمراجعة هذه العملية تبين أن عملية التعرف الذي أجراها مكتب التحقيقات الفيدرالي كانت مبنية على صور ذات جودة رديئة أظهرت عددًا كبيرًا من نقاط التشابه بين مجموعتي البصمات^(١٠٦).

وتعتمد الموثوقية على عدة عوامل منها: إمكانية جمع عينات حيوية عالية الجودة، استقرار السمة الحيوية، التي يُمكن أن تتغير بمرور الوقت؛ بسبب التقدم في السن، أو الإصابة بجرح عميق؛ فالتغيرات الحاصلة في الخصائص الحيوية قد تُعيق الاعتماد عليها، فلا تُعد الخصائص الحيوية للأطفال – على سبيل المثال

، مرجع سابق، (WP96) Article 29 Data Protection Working Party in WP 29 Opinion 7/2004 on VIS (102) ص 6.

(103) Charter of Fundamental Rights of the European Union [2012] OJ C326/391, art 48(2); Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR), art 6(3); International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR), art 14.

(104) Charter of Fundamental Rights of the European Union [2012] OJ C326/391, arts 25 and 26.

(105) GDPR, Art.22 (3).

(106) Federal Bureau of Investigation, Statement on Brandon Mayfield Case (24 May 2004) <https://archives.fbi.gov/archives/news/pressrel/press-releases/statement-on-brandon-mayfield-case>

موثوقةً في بعض الحالات؛ حيث تحتاج هذه البيانات إلى تحديثٍ مع مرور الوقت؛ نتيجةً لنضج الخصائص، وقد تُواجهُ بعضُ الفئات السكانية؛ (مثل العمال أصحاب الحرف اليدوية، ذوي الإعاقة) صعوبةً في توفير عيّناتٍ موثوقة؛ نتيجةً لضعف السمات الحيوية المُميزة (١٠٧).

كما يعتمد التوفّر على إمكانية استخدام التطبيق في بيئاتٍ متنوّعة؛ حيث تقلل بعض الظروف الجوية؛ مثل درجات الحرارة العالية، وكذلك العوامل البيئية من توفّر هذه التقنية.

وللحدّ من تلك العيوب، يُمكن استخدام عدّة حلول؛ منها: استخدام أغلفة مقاومة للعوامل الجوية لحماية أجهزة المسح الحيوي، استخدام أحدث إصدارات أنظمة القياس الحيوي، تطبيق إجراءات احتياطية (بديلة)؛ لتحديد الهوية لدعم أنظمة القياس الحيوي حال ثبوت عدم موثوقيتها

خامساً: المخاطر الأمنية:

تكتسب الجوانب الأمنية أهميةً بالغة بالنسبة إلى أنظمة القياسات الحيوية؛ فإذا كان الهدف الرئيس لاستخدام هذه التقنيات هو تعزيز الأمن، من خلال توفير رابط قوي مع صاحب البيانات؛ إلا أنه يجب الاعتراف بأن أنظمة القياس الحيوي؛ باعتبارها أنظمة معلومات واتصالات، تكون عُرضةً كذلك للثغرات الأمنية والهجمات السيبرانية في كافّة مراحل تشغيلها؛ كما هو الحال في أيّ نظام تكنولوجيا معلومات، لذا يجب - التزاماً بمبدأ أمن البيانات «Data Security»؛ باعتباره أحد المبادئ الأساسية لمعالجة البيانات الشخصية وفقاً للمادة (٥) من اللائحة العامة لحماية البيانات (GDPR) (١٠٨) - حماية هذه البيانات في كل مرحلة من مراحل المعالجة؛ ابتداءً من جمع البيانات، وانتهاءً باتخاذ القرار النهائي بشأنها؛ لذلك تتطلب جميع أنظمة القياسات الحيوية سياسةً أمنية صارمة، وإجراءات مُعقّدة وفقاً للمعايير الدولية

وتتخذ هذه المخاطر عدّة صور أهمها:

١ - هجمات أنظمة التقاط البيانات:

تلتقط أنظمة القياسات الحيوية الخصائص الحيوية من صاحب البيانات للتسجيل، أو الاستخدام لاحقاً (المقارنة)، وأثناء التسجيل، وكذلك المقارنة اللاحقة؛ يجب أن تكون العيّنة الحيوية مُستخرجةً من صاحب البيانات الحقيقي (١٠٩).

(107) World Bank, Practitioner's Guide: Biometric Data, Identification for Development (ID4D) <https://id4d.worldbank.org/guide/biometric-data>

(108) GDPR, Art.5 (1) (f).

(109) Els J Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Springer 2013) 369.

ومع ذلك، يمكن تقديم خصائص حيوية مُزيّفة إلى جهاز استشعار القياسات الحيوية؛ بما في ذلك الخصائص الحيوية للآخرين؛ فقد يُجبرُ شخصٌ ما على تقديم بياناته الحيوية وهو ما يُسمّى «الهجوم القسري»، كما قد يتمّ تغيير مظهر الشخص لتقليد السمات الحيوية لشخصٍ آخر؛ وهو ما يُطلقُ عليه «انتحال الهوية»^(١١٠) الذي يتّخذُ عدّة صور؛ منها: إنشاء «نسخة مُزيّفة»، أو نسخة مُكرّرة مُزيّفة للوصول غير المُصرّح به؛ فعلى سبيل المثال: هناك تقنية تُسمّى «تحريف الوجه» تعتمد على مسح الوجه، وتقديم صورة مُعدّلة على وثيقة رسمية – الصورة المُعدّلة عبارة عن تجميع لملامح شخصين مختلفين في صورة واحدة – مما يسمح لأيٍّ منهما باستخدام الهوية الرسمية دون كشف هويّته^(١١١).

ونظرًا لشيوع هجمات انتحال الهوية، فقد جرى اقتراحُ بعض الأساليب للتغلّب على تلك الهجمات؛ منها:

- كشف الهوية الحيوية: استخدام التقنيات للتحقق من أن العيّنة الحيوية مُستخرّجة من شخصٍ حي، وتتّخذُ هذه الطريقة إحدى صورتين: (الأولى: الكشف الإيجابي عن الهوية الحيوية: الذي يتطلب تفاعلاً من المُستخدم كالابتسام مثلاً)، (الثانية: الكشف السلبي عن الهوية الحيوية: يستخدم تحليلًا مُتقدّمًا لخصائص معيّنة؛ مثل: ملمس الجلد، قياس درجة حرارة الجسم، نبض الدم)^(١١٢).
- اختبار العلاقة بين الشخص والبيانات الملتقطة: بالنسبة إلى أنظمة بصمات الأصابع قد يُصنّف استخدام أصابع مُتعدّدة (بتسلسل مُحدّد) القدرة على الانتحال.
- الإشراف على مواقع جمع البيانات.
- تركيب كاميرات في مواقع النقاط البيانات.
- استخدام أنظمة قياس حيوي مُتعدّدة الوسائط (تستخدم سمات حيوية مُتعدّدة).
- المصادقة مُتعدّدة العوامل: دمج القياسات الحيوية مع طرق المصادقة الأخرى لتعزيز الأمان.

(١١٠) المرجع السابق، ذات الموضوع.

(111) RSS Kramer, MO Mireku, TR Flack and others, 'Face Morphing Attacks: Investigating Detection with Humans and Computers' (2019) 4 *Cognitive Research* 28 <https://doi.org/10.1186/s41235-019-0181-4>

(112) S Khairnar, S Gite, K Kotecha and SD Thepade, 'Face Liveness Detection Using Artificial Intelligence Techniques: A Systematic Literature Review and Future Directions' (2023) 7(1) *Big Data and Cognitive Computing* 37 <https://doi.org/10.3390/bdcc7010037>

وهناك أيضًا ما يُسمّى بهجمات «الالتقاط وإعادة التشغيل»؛ ويُقصدُ بها تلك التي يتمّ فيها اعتراض إرسال بيانات حيويّة صحيحة وتسجيلها - من خلال الشبكة، وإعادة تشغيلها لاحقًا للحصول على وصول غير مُصرّح به

وتجدر الإشارة إلى أنه يُشترطُ أن يكون جهاز النقاط البيانات «المُستشعر» موثوقًا؛ وهو ما يعني أن يكون قادرًا على التواصل بشكل آمن مع باقي المحتويات الماديّة للنظام؛ مما يتطلّب استخدام مفاتيح تشفير وإدارة المفاتيح لمصادقة الجهاز، بالإضافة إلى ذلك، يجبُ أن يكون الجهاز مُقاومًا للتلاعب^(١١٣)؛ بحيث يكون مُصمّمًا بطريقة تمنع الوصول غير المصرّح به، وتُظهرُ بوضوح ما إذا كان أحدهم يحاول العبث به؛ مما يتطلّب تنفيذ تدابير ماديّة وتقنيّة مُعقّدة، وبشكل عام؛ تطلّ الرقابة البشريّة الكافية لبعض أنظمة القياس الحيوي الطريقة الفعّالة الوحيدة للحدّ من مخاطر هجمات النقاط البيانات «المُستشعر»^(١١٤).

٢- الهجمات أثناء عمليّة «استخراج السمات والمقارنة»:

تُعَدُّ عمليّة استخراج السمات «معالجة الإشارة»، وكذلك نظام المقارنة الفرعي في تقنيّات القياسات الحيويّة عُرضةً لبيانات مزيفة من خلال هجمات يُطلَقُ عليها اسم «حصان طروادة - Trojan horse»؛ ويهدف هذا النوع من الهجمات إلى تجاوز وظائف إحدى المكونات، أو التلاعب بها؛ والذي قد يشمل: استبدال برنامج كشف السمات، و/ أو خوارزميات المقارنة

ومن الصور الأخرى لهذه الهجمات: تعديل درجات المقارنة، وللحدّ من هذه الهجمات يُمكنُ اعتماد التثبيّت، واستخدام تدابير أمنيّة خاصّة بهذه المكونات

٣- الهجمات على وسائط التخزين «مركزيّة أو محليّة»:

هناك نوع من التهديدات يتعلّق بنظام تخزين البيانات الفرعي؛ والذي يُمكنُ مهاجمته أيضًا عن طريق تمكّن أشخاص غير مُصرّح لهم من الوصول إلى بيانات القياس الحيوي المرجعيّة، أو تغييرها، أو استبدالها، أو سرقتها، ولا تقتصرُ عواقبُ هذا التهديد على أمن النظام فحسب؛ بل تمتدُّ إلى الخصوصية بشكل عام

لذا تُعَدُّ الحماية الكافيّة لجميع مُكوّنات تخزين نظام القياس الحيوي متطلّبًا أساسيًا، والتي ستكون أكثر صعوبة بالنسبة للبيانات الحيويّة المُخزّنة مركزيًا؛

(113) Michael Gasson, Martin Meints and Kevin Warwick (eds), *D3.2 A Study on PKI and Biometrics*, FIDIS (2005) <http://www.fidis.net/resources/fidis-deliverables>

(١١٤) Kindt, Els J.، مرجع سابق، ص ٣٧٠.

مقارنةً بنظيرتها المخزنة محليًا؛ ولهذا السبب يُفضَّلُ التخزينُ المحلي على بطاقةٍ ذكيَّةٍ مثلاً

وللحدِّ من هذه الهجمات يُمكنُ اتِّخاذ تدابيرٍ أمنيَّةٍ؛ مثل تخزين البيانات في وحدات تخزينٍ مقاومة للعبث، لا تقبل التخزينَ أكثرَ من مرة واحدة فقط

٤- الهجمات على نظام اتِّخاذ القرار:

هناك نوعٌ آخر من الأخطار يستهدف نظام اتِّخاذ القرار الفرعي لتعديل النتائج؛ فهذا النظام عُرضةٌ لما يُسمَّى بهجمات «تسلُّق التِّل - hill climbing»، والتلاعب بنقطة المقارنة^(١١٥)؛ ففي هجمات «تسلُّق التِّل» يتمُّ تعديل المُدخَّلات الحيويَّة تدريجيًّا لتحسين نتيجة المقارنة، حتى تحقيق تطابقٍ ناجح، أما في حالة التلاعب بنقطة المقارنة؛ فيقوم المهاجم بتعديل نقطة المقارنة للحصول على نتيجة إيجابِيَّة، ويستلزم هذا النوع من الهجمات اتِّخاذ تدابير مناسبة

٥- الهجمات أثناء عمليَّة نقل البيانات:

تتكون الأنظِمة الحيويَّة من عناصر مختلفة، ويتطلَّب التواصل بين هذه العناصر وجود قنوات اتصال وإرسال؛ ومن ثم فإن الأنظِمة المفتوحة المُورَّعة في أماكن عديدة تكون أكثرَ عُرضَةً للتَنصُّت - الاستماع سرًّا إلى اتصال خاص دون موافقة -، وهو ما يُطلَقُ عليه «هجمات الوسيط - man-in-the-middle» و«القوة الغاشمة - brute force» وتعني تجربة أي تركيبة وكل شفرة ممكنة للوصول إلى البيانات المُستهدَفة^(١١٦).

وللحدِّ من هذا النوع من الهجمات يُمكنُ تطبيق العديد من الحلول؛ منها: تطبيق تقنيَّات اتصال آمنة، تشفير المعلومات المُرسلة، تقليل الوصول إلى البنية التحتيَّة الماديَّة، استخدام رموز الجلسة من خلال عمليَّة عشوائيَّة، المراقبة الشاملة للبنية التحتيَّة

(115) M Bromba, 'Reconstruction of Biometric Raw Data' (2006); J Breebaart, B Yang, I Buhan-Dulman and C Busch, 'Biometric Template Protection' (2009) 301.

(١١٦) Kindt, Els J.، مرجع سابق، ص ٣٧٢.

المبحث الثالث التنظيم القانوني لأنظمة التعرف الحيوي في قانون الذكاء الاصطناعي «AI Act»

في فبراير من عام ٢٠٢٠، أصدرت المفوضية الأوروبية وثيقة بعنوان (تشكيل مستقبل أوروبا الرقمي-Shaping Europe's Digital Future)؛ أشارت من خلالها إلى ضرورة تطوير أطر تنظيمية متوازنة تُعزِّز الثقة بالذكاء الاصطناعي، وتدعم استخداماته المسؤولة^(١١٧)، كما أصدرت (الورقة البيضاء حول الذكاء الاصطناعي- White Paper on Artificial Intelligence)، والتي حدّدت أهدافاً لضمان الريادة الأوروبية في هذا المجال التكنولوجي، وتحقيق التوازن بين استخدام الذكاء الاصطناعي، وحماية حقوق مواطني الاتحاد الأوروبي، واعترفت من خلالها بالانتهاكات الخطيرة المحتملة للحقوق الأساسية الناتجة عن استخدام الذكاء الاصطناعي، ودعت إلى وضع إطار تنظيمي يُقلِّل من المخاطر المحتملة^(١١٨).

وفي أبريل من عام ٢٠٢١، قدّمت المفوضية الأوروبية رسمياً (اقتراح قانون الذكاء الاصطناعي - Proposal AI Act)^(١١٩)، كما قدّمت الجهات الممثلة في (البنك المركزي الأوروبي - لجنة المناطق - اللجنة الاقتصادية والاجتماعية) آراءها بشأن هذا المقترح، وبتاريخ ١٣ مارس عام ٢٠٢٤، صوّت البرلمان الأوروبي بالموافقة على الصيغة النهائية لقانون الذكاء الاصطناعي، وأقرّ - لاحقاً - تعديلات لهذا المقترح التشريعي^(١٢٠).

وبتاريخ ٢١ مايو عام ٢٠٢٤، تمّ توقيع قانون الذكاء الاصطناعي رسمياً، ونُشر - بتاريخ ١٢ يوليو عام ٢٠٢٤ - في الجريدة الرسمية للاتحاد الأوروبي «Official Journal of the EU»، ودخل حيّز التنفيذ؛ اعتباراً من ١ أغسطس عام ٢٠٢٤.

(117) European Commission, *Shaping Europe's Digital Future* (February 2020) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0067>

(118) European Commission, *White Paper on Artificial Intelligence – A European Approach to Excellence and Trust*, COM(2020) 65 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0065>

(119) European Commission, *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, COM/2021/206 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>

(120) Future of Life Institute, 'The Act Texts' (Future of Life Institute, 2024) <https://artificialintelligenceact.eu/theact/>

أولاً: أهدافه الرئيسية:

تُمثِّلُ تقنيَّات الذكاء الاصطناعي فرصةً كبيرة لتحسين جودة الحياة في العديد من المجالات؛ مثل الرعاية الصحية، الخدمات العامة، والتي تُعزِّزُ - حالَ تطويرها - القدرة التنافسيَّة العالمية للاتِّحاد الأوروبي؛ إلا أنه وفي الوقت ذاته، فإنَّ هذه التقنيَّات قد تضرُّ بالحقوق الأساسيَّة لمواطني الاتحاد الأوروبي^(١٢١).

لذا؛ يتمثِّلُ الهدف الأساسي من إقرار قانون الذكاء الاصطناعي في إنشاء إطار تنظيمي مُنسِّق بين الدول الأعضاء في الاتحاد الأوروبي لتطوير الذكاء الاصطناعي، وطَّرحه في الأسواق، ونشره واستخدامه على نطاقٍ واسع، كما يسعى إلى تشجيع الابتكار في هذا المجال بطريقةٍ تضمَّنُ حماية صحَّة المواطنين وسلامتهم وحقوقهم الأساسيَّة المنصوص عليها في ميثاق الحقوق الأساسيَّة للاتِّحاد الأوروبي

ثانياً: نطاق تطبيقه:

اتَّخذ قانون الذكاء الاصطناعي نطاقاً شخصياً واسعاً يشمل ستَّ فئات؛ هم: المُورِّدون، والمُورِّعون، والمستوردون، ووكلاء التوزيع، ومُصنِّعو المنتجات، والممثِّلون المُفوضون - ويُستخدَمُ مصطلح "المُشغِّل" لوصفهم جميعاً^(١٢٢)، ويُعرَّف معظم المُشغِّلين بالإشارة إلى ثلاث مصطلحاتٍ رئيسة مُقتبسة من تشريعات الاتحاد الأوروبي المُشار إليها في المُلحق الأول من قانون الذكاء الاصطناعي: "الإتاحة"، و"الطرح في السوق"، و"التشغيل"

"الإتاحة" هي توفير نظام ذكاء اصطناعي، أو نموذج ذكاء اصطناعي للأغراض العامة للتوزيع، أو الاستخدام في سوق الاتحاد الأوروبي في سياق نشاطٍ تجاري؛ سواءً بمقابل أو مجاناً؛ و"الطرح في السوق" هو أول إتاحة لنظام ذكاء اصطناعي، أو نموذج ذكاء اصطناعي للأغراض العامة في سوق الاتحاد الأوروبي؛ و"التشغيل" هو توفير نظام ذكاء اصطناعي للاستخدام الأول مباشرةً للجهة المُستخدمة، أو للاستخدام الخاص في الاتحاد الأوروبي للأغراض المقصودة منه

وتجدرُ الإشارةُ إلى أن قانون الذكاء الاصطناعي لم يبيِّن مفهوم "الاستخدام"؛ لذا يمكن تعريف هذا المصطلح من خلال الوظيفة الرئيسة له في أنظِمة الذكاء الاصطناعي على أنه "استنتاج كيفية توليد المُخرجات من المدخلات التي يتلقاها النظام"

(121) AI Act, Recital 4-5.

(122) AI Act, Article 2 (1) (a-g).

ويُقصدُ بمصطلح «المزود»: أيُّ شخصٍ طبيعي أو اعتباري؛ بما ذلك السلطات العامّة، أو الوكالات، أو أي هيئاتٍ أخرى تُطوّرُ نظام ذكاء اصطناعي، أو نموذج ذكاء اصطناعي للأغراض العامّة، أو تمتلك نظام ذكاء اصطناعي، أو نموذج ذكاء اصطناعي مُطوّر للأغراض العامّة، تطرحه داخل السوق، أو تشغله باسمها الخاص، أو علامتها التجاريّة؛ سواء كان ذلك بمقابل، أو دون مقابل (١٢٣).

وعلى الرغم من أن مصطلح «الطرح داخل السوق» يُشير إلى سوق الاتّحاد الأوروبي؛ إلا أنه لا يزال من الممكن اعتبار الشخص «مُزوّدًا» يخضع لأحكام القانون، ولو لم يقدّم بطرح نظام ذكاء اصطناعي داخل سوق الاتّحاد الأوروبي؛ بل يكفي قيامه باستخدام مُخرجات نظام ذكاء اصطناعي داخل الاتّحاد الأوروبي

كما يُقصدُ بمصطلح «الموزّع»: أي شخص طبيعي أو اعتباري، بما ذلك السلطات العامّة، أو الوكالات، أو أي هيئاتٍ أخرى تُستخدِمُ نظام ذكاء اصطناعي تحت سُلطتها (١٢٤)؛ ومن ثمّ فقد استُبدِلَ مصطلح «المُستخدِم – User» الذي استُخدِمَ سابقًا في الاقتراح الأول للمفوضيّة الأوروبيّة برغم عدم تغيير المقصود بهذا المصطلح (١٢٥)، وهناك استثناءات للاستخدام العسكري، ولأغراض البحث العلمي، وكذلك للاستخدام الشخصي (غير المهني) (١٢٦).

ويُقصدُ بمصطلح «المستورد»: أي شخص طبيعي أو اعتباري يتواجد، أو يقيم داخل الاتّحاد، ويقوم بطرح نظام ذكاء اصطناعي داخل سوق الاتّحاد الأوروبي يحمل اسمًا، أو علامةً تجاريّةً لشخصٍ طبيعي، أو اعتباري مُقيم في دولةٍ أخرى

كما يُقصدُ بمصطلح «وكيل التوزيع»: أي شخص طبيعي أو اعتباري في سلسلة التوريد، بخلاف المُورّد أو المستورد؛ يُسهّم في جعل نظام الذكاء الاصطناعي متاحًا داخل سوق الاتّحاد الأوروبي

وفيما يتعلّق بالنطاق المادي للقانون: ينطبق قانون الذكاء الاصطناعي على «أنظمة الذكاء الاصطناعي»؛ ونظرًا لصعوبة تعريف «الذكاء الاصطناعي»؛ فقد اختار مشرعو الاتّحاد الأوروبي مفهومًا واسعًا يتسم بالمرونة بالتنسيق مع المنظمات الدوليّة العاملة في مجال التكنولوجيا (١٢٧)،

(123) AI Act, Art 3 (4).

(124) AI Act, Ibid.

(125) European Commission, *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM(2021) 206 final.

(126) AI Act, article 2 (3), (6), (8), (10).

(127) AI Act, Recital 12.

وَتُعَرَّفُ «نظم الذكاء الاصطناعي» على أنها نظم آلية ذات مستويات متفاوتة من الاستقلالية والقدرة على التكيف، ولديها القدرة على «الاستدلال» من خلال المدخلات التي تتلقاها لتوليد مخرجات (تنبؤات، محتوى، توصيات، قرارات) (١٢٨).

وقد ركّز هذا التعريف على التمييز بين أنظمة الذكاء الاصطناعي والبرامج التقليدية من خلال تسليط الضوء على القدرة على الاستدلال، التي تشمل القدرة على التعلم والاستنتاج، وتحقيق من خلال التعلم الآلي (١٢٩).

وفيما يتعلّق بالنطاق الإقليمي: تنطبق أحكام قانون الذكاء الاصطناعي عندما يكون نظام الذكاء الاصطناعي؛ سواء كان مستقلاً، أو جزءاً من منتج خاضع لتشريعات سلامة المنتجات في الاتحاد الأوروبي في الملحق الأول:

- يُطْرَحُ أو يُشْعَلُ أو يُسْتَوْرَدُ أو يُوزَعُ داخل الاتحاد الأوروبي.
- يُسْتَحْدَمُ من قِبَل جهة نشر تتواجد، أو لها مقر داخل الاتحاد الأوروبي.

وتنطبق أحكام البند الأول، بغض النظر عن المقر الذي يتّخذه «مزود» نظام الذكاء الاصطناعي، وسواء كان هذا المقر داخل أو خارج الاتحاد، ونظراً لخلوّ قانون الذكاء الاصطناعي من بيان لمصطلح «المقر»؛ فمن المتوقع أن يجري تفسير هذا المصطلح على النحو الذي يجري عليه العمل في تشريعات الاتحاد الأوروبي الأخرى؛ مثل اللائحة العامة لحماية البيانات

بالإضافة إلى ما تقدّم، تُطبّق أحكام قانون الذكاء الاصطناعي أيضاً إذا استُخدمت مخرجات نظام ذكاء اصطناعي خارج الاتحاد الأوروبي في داخل الاتحاد الأوروبي، وفي هذه الحالة، سيخضع مُقدِّمُ الخدمات، والناشرون المتواجدون خارج الاتحاد الأوروبي أيضاً لنطاق قانون الذكاء الاصطناعي

ثالثاً: تصنيف أنظمة الذكاء الاصطناعي (النهج القائم على المخاطر):

اتّبع قانون الذكاء الاصطناعي نهجاً واضحاً قائماً على المخاطر من خلال تكييف الأحكام واجبة التطبيق مع نطاق المخاطر المحتملة التي يُشكّلها نظام الذكاء الاصطناعي المعني؛ لذلك تُصنّف أنظمة الذكاء الاصطناعي - وفقاً لمخاطرها المقدّرة مسبقاً- إلى فئات مُتعدّدة (١٣٠).

(128) AI Act, Art 3 (1).

(129) AI Act, Recital 12.

(130) AI Act, Recital 26.

وقد قسّم قانون الذكاء الاصطناعي هذه الأنظمة إلى أربع فئات:

الذكاء الاصطناعي ذو المخاطر غير المقبولة «Unacceptable risk»: لا يُسمح باستخدامها إطلاقاً – وفقاً للباب الثاني من التشريع –؛ إلا أن القانون نصّ على بعض الاستثناءات؛ مثل «التقييم الاجتماعي»

الذكاء الاصطناعي عالي المخاطر «High risk»: يُسمح باستخدام هذه الأنظمة، ولكنّها تخضع لمعايير صارمة؛ بما في ذلك: تقييمات المطابقة؛ حيث يجب أن تجتاز تقييم مطابقة يجري عليها قبل طرحها في الأسواق، كما تخضع لمراقبة دقيقة أثناء التشغيل⁽¹³¹⁾.

الذكاء الاصطناعي منخفض المخاطر «Limited risk»: لا يُشترط فيها سوى التزامات محدّدة تتعلّق بالشفافية؛ (مثل برامج الدردشة الآليّة - Chatbots، التزييف العميق - deep fakes)

الذكاء الاصطناعي ذو المخاطر الضئيلة «Minimal or no risk»: لا يخضع هذا النوع من الأنظمة إلى أيّ قيود تنظيميّة بموجب قانون الذكاء الاصطناعي

رابعاً: تطبيق قانون الذكاء الاصطناعي على أنظمة التعرف الحيوي عن بُعد:

تُعتبر أنظمة التعرف الحيوي عن بُعد المدعومة بالذكاء الاصطناعي من أنظمة الذكاء الاصطناعي، وتخضع – من ثمّ – إلى قانون الذكاء الاصطناعي، وتُصنّف الأنظمة الأكثر شيوعاً منها على أنها أنظمة ذات مخاطر غير مقبولة، أو عالية المخاطر، ولتحديد القواعد واجبة التطبيق على نظام تعرّف حيويّ مُعيّن، يجب التمييز بين خصائص التعرف، التحقق، والتصنيف بالإضافة إلى تحديد الهوية «الفوري» أو «اللاحق» علاوة على تقييم لسياق الاستخدام⁽¹³²⁾

خامساً: أنشطة الذكاء الاصطناعي المحظورة:

تناول الفصل الثاني من قانون الذكاء الاصطناعي ممارسات الذكاء الاصطناعي المحظورة، والتي قدّر المشرعون تعارضها مع قيم الاتحاد الأوروبي، واعتبروها تهديداً واضحاً للحقوق الأساسية؛ كالحريّة، والمساواة، والخصوصيّة⁽¹³³⁾؛ ومن ثمّ فقد مثلت هذه المحظورات محاولة من جانب هؤلاء المشرعين للاستجابة للمخاوف المتعلّقة بالشفافية، وبهدف ضمان حماية حقوق الإنسان،

(131) Tambiama Madiega and Hendrik Mildebrath, Regulating Facial Recognition in the EU (European Parliamentary Research Service 2021) [https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA\(2021\)698021_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf)

(132) Ibid.

(133) AI Act, Recital 32.

تناولت المادة (5) من القانون^(١٣٤) الممارسات المحظورة بشكلٍ شامل، ووضعت إطاراً واضحاً لما يُمكنُ للذكاء الاصطناعي فعله، وما لا يُمكنه فعله داخل الاتحاد الأوروبي

وقد اكتسب الحظرُ المنصوص عليه في المادة (5) أهميةً خاصّة برّرت أسبقية دخوله حيّز النفاذ، مقارنةً بسائر أحكام القانون الأخرى؛ حيث دخل بالفعل حيّز النفاذ؛ اعتباراً من ٢ فبراير عام ٢٠٢٥، وتجدر الإشارة إلى أنّ قائمة الأنشطة المحظورة الواردة في المادة (٥) ليست نهائية؛ حيث تخضع لتقييم سنوي من قبل المفوضية الأوروبية – تطبيقاً لنص المادة (١١٢) من القانون – ويُقدّم هذا التقييم إلى البرلمان والمجلس الأوروبيين؛ لذا قد يطرأ تغييرٌ في الأنشطة المحظورة بمرور الوقت نتيجةً لهذا التقييم

وتضمّنت المادة (٥) ثماني ممارسات؛ ركّزت على الأنشطة التي من شأنها تحريف سلوك الأفراد بشكلٍ ملموس، أو تلك التي تُؤثّر على حقوق الأفراد بشكل كبير، كما أولت اهتماماً كبيراً بأنظمة تحديد الهوية الحيوية، إلا أنه – ومع ذلك – فقد تضمّن القانون استثناءاتٍ مُفصّلة للعديد من الأنشطة المحظورة

وسوف نستعرض فيما يلي هذه الممارسات بشيءٍ من التفصيل:

١ - التقنيّات الخفية أو الخادعة^(١٣٥):

يتعلّق الحظر الأول بأنظمة الذكاء الاصطناعي التي تُستخدم تقنيّات خفية أو خادعة في الحالات التالية:

- أن تهدف التقنية إلى تشويه سلوك فرد، أو مجموعة من الأفراد، أو يكون لها تأثير فعلي عليهم.
- الإضرار الكبير بقدرة الأفراد على اتّخاذ قرارات مستنيرة.
- إجبار الأفراد على اتّخاذ قرارات لم يكونوا ليتّخذوها لولا ذلك، والتي تُسبّب، أو يُحتمل أن تُسبّب ضرراً جسيماً لهم.

(134) AI Act, Art 5.

(135) AI Act, Art 5 (1) A.

وتتضمّن هذه الأساليب – وفقاً لما أشارت إليه الفقرة ٢٩ من القانون (١٣٦) - استخدام محفّزات صوتيّة، صور، مقاطع فيديو لا يستطيع الشخص إدراكها، أو أساليب خادعة تنال من استقلاليّة الفرد، وتُقيّض من قدرته على اتّخاذ القرار المناسب بطرق تجعل الأفراد لا يدركون هذه الأساليب، وفي حال إدراكهم لها لا يستطيعون مُقاومتها، أو السيطرة عليها، وتُستخدَم هذه الأساليب عادةً من خلال: الواجهات الآليّة، الواقع الافتراضي؛ لأنها تسمح بدرجة أعلى من التحكم في المحفّزات المقدمة للأشخاص

٢- استغلال الفئات المعرّضة للخطر (١٣٧):

تهدف الفئة الثانیّة من ممارسات الذكاء الاصطناعي المحظورة إلى حماية الفئات الأكثر عرضة للخطر – وهي ما تُسمّى بالفئات الضعيفة-، والتي تنقسم إلى ثلاثة أقسام؛ هي: الفئات الضعيفة نتيجةً للسن، أو الإعاقة، أو بسبب أوضاع اقتصاديّة، أو اجتماعيّة محدّدة

ولكي يتمّ حظر هذه الفئة من فئات الذكاء الاصطناعي يلزم وجود شرطين؛ هما:

- أن تهدف التقنية إلى تشويه سلوك فرد بشكل ملموس.
- أن يتمّ ذلك بطريقة تُسبّب أو يُحتمل أن تُسبّب ضرراً جسيماً لشخص ما.

فعلى سبيل المثال؛ قد يُستخدَم الذكاء الاصطناعي لاستهداف الأفراد من ذوي الاحتياجات الخاصّة لأغراض الاستغلال الاقتصادي، لذا يجب على المنظمات التي تستخدم أنظمة الذكاء الاصطناعي للتسويق والمبيعات أن تتحقّق من اختبار أنظمتها لمنع ذلك

وتجدر الإشارة إلى أنّ هذه الفئة تشترك مع الفئة الأولى المتعلّقة بالتقنيّات الخفيّة في اشتراط وجود «ضرر جسيم»، وهو مفهوم شاملٌ يتضمّن أكثر من مجرد ضرر جسدي أو نفسي، ومع ذلك؛ فقد تضمنت الفقرة ٢٩ من القانون أمثلة على هذا الضّرر؛ شملت: أضراراً بدنيّة، نفسيّة، مصالح الماليّة، وكذلك الأضرار التي تتراكم بمرور الوقت

(136) AI Act, Recital 29.

(137) AI Act, Art 5 (1) B.

٣- التقييم الاجتماعي^(١٣٨):

تتعلق هذه الفئة بما يُسمّى «التقييم الاجتماعي»، ويُقصدُ به: تصنيف الأفراد، أو المجموعات على نطاقٍ زمنيٍّ مُحدّد؛ بناءً على سلوكهم الاجتماعي، أو خصائصهم الشخصية المُستنتجة

ويحظر التقييم الاجتماعي في حالتين هما:

• إذا أدّى هذا التقييم إلى معاملة غير مُناسبة في سياقات اجتماعية لا علاقة لها بالسياق الذي وُجِدَت فيه البيانات في الأصل.

• إذا أدّى ذلك التقييم إلى معاملة غير مُناسبة للأفراد أو المجموعات بشكل غير مُبرّر، أو غير مُتناسب مع سلوكهم الاجتماعي أو خطورته.

وقد استُخدِمَ التقييم الاجتماعي من قِبَل العديد من حكومات الدول حول العالم؛ ففي عام ٢٠٢١ استقالت الحكومة الهولندية؛ نتيجة استخدامها خوارزمية تقييم اجتماعي معيبة؛ ترتّب على استخدامها اتهام بعض الفئات ظلماً بالاحتيال على نظام الرعاية الاجتماعية

وينطبق هذا الحظر على جميع أنظمة التقييم الاجتماعي؛ بما في ذلك أنظمة التقييم الاجتماعي التي تُطبّقها جهاتٌ خاصّة، كما يستهدف عواقب التقييم، وليس التقييم في حدّ ذاته؛ بمعنى أن التقييم الذي يستهدف القانون حظره هو ذلك النوع الذي يُؤدّي استخدامه إلى نتائج غير عادلة «تمييزية»

٤- استخدام السمات الشخصية لتقييم المخاطر الجنائية^(١٣٩):

يُحظر طرح أو تشغيل أو استخدام أنشطة الذكاء الاصطناعي التي تنتبأ باحتمالية ارتكاب شخصٍ ما لجريمة؛ بناءً على تقييم السمات الشخصية فقط

ويُسْتَنَتَى من هذا الحظر أنظمة الذكاء الاصطناعي المُستخدمة لدعم التقييم البشري في استنتاج تورُّط شخصٍ ما في نشاطٍ إجرامي، والتي تستند إلى حقائق موضوعية قابلة للتحقق ترتبط ارتباطاً مباشراً بنشاطٍ إجرامي – ويُقصدُ بها أدوات الكشف الواقعية التي تُكمل عملية صنع القرار البشري دون أن تحلّ محلها

(138) AI Act, Art 5 (1) C.

(139) AI Act, Art 5 (1) D.

يُحظرُ طرح، أو تشغيل، أو استخدام أنشطة الذكاء الاصطناعي لإنشاء أو توسيع قواعد بيانات التعرف على الوجه من خلال استخراج صور الوجه من الإنترنت، أو الكشف غير المستهدف لصور الوجه من خلال لقطات كاميرات المراقبة

وقد بيّنت الفقرة (٤٣) من القانون^(١٤١) الحكمة من هذا الحظر؛ والتي تتمثل في مساهمة هذه الممارسة في مُفاقمة الشعور بالمراقبة الجماعية؛ الأمر الذي قد يترتب عليه حدوث انتهاك للحقوق الأساسية للفرد؛ أهمها الحق في الخصوصية

وقد يضع هذا الحظر حدًا للممارسات الملثوية التي تُطبّقها شركات تطوير أنظمة الذكاء الاصطناعي؛ مثل Clearview AI، PimEyes التي تقوم باستخراج أعدادٍ لا حصر لها من صور الوجه الموسومة باسم الشخص المعني من مواقع الويب المختلفة دون موافقة الأشخاص أصحاب البيانات^(١٤٢).

ويُعزّر ذلك اشتراط تقديم وثائق فنيّة مُفصّلة قبل طرح نظام الذكاء الاصطناعي في السوق، والتي يجب أن تتضمّن، من بين أمورٍ أخرى، معلوماتٍ عن طرق الحصول على بيانات تدريب الأنظمة ومصدرها^(١٤٣).

٦- استنباط المشاعر في أماكن العمل أو المؤسسات التعليمية^(١٤٤):

يُحظرُ طرح، أو تشغيل، أو استخدام أنشطة الذكاء الاصطناعي لاستنباط المشاعر في أماكن العمل، أو المؤسسات التعليمية إلا لأغراض السلامة أو الأسباب الطبية؛ مثل الأنظمة المُخصّصة للاستخدام العلاجي

وقد بيّنت الفقرة (١٨) من القانون^(١٤٥) المقصود بالمشاعر على أنها: «حالة داخلية؛ كالسعادة، والحزن، والغضب»؛ وبالتالي يخرج عن هذا المفهوم:

(140) AI Act, Art 5 (1) E.

(141) AI Act, Recital 43.

(142) Amba Kak, Regulating Biometrics: Global Approaches and Open Questions (AI Now Institute 2020) <https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions>

(143) Article 11 AI Act referring to Annex IV AI Act.

(144) AI Act, Art 5 (1) F.

(145) AI Act, Recital 18.

• الحالات الجسدية؛ كالآلم أو التعب؛ ومن ثم لن تتأثر الأنظمة المستخدمة في الكشف عن حالة التعب لدى الطيارين، أو السائقين المحترفين بغرض منع الحوادث.

• التعبيرات الواضحة كالابتسام، أو العبوس، أو الإيماءات كحركة اليدين، أو الذراعين، أو الرأس، أو خصائص صوت الشخص؛ كالصوت المرتفع، أو الهمس

ويعرّف قانون الذكاء الاصطناعي مُصطلح «نظام التَّعرُّف على المشاعر» على أنّه «نظام ذكاء اصطناعي يُستخدَم لغرض تحديد، أو استنتاج مشاعر، أو نوايا الأشخاص الطبيعيين؛ بناءً على بياناتهم الحيوية»^(١٤٦).

ومن الجدير بالذكر أن المادة (٥) (و) استخدمت مصطلح «أنظمة الذكاء الاصطناعي لاستنتاج المشاعر»؛ ممّا مؤداه أن الحظر يشمل كافة الأنظمة دون اشتراط استخلاص المشاعر من البيانات الحيوية، إلا أنّ الفقرة (٤٤) من القانون أكّدت على أن تطبيق المادة (٥) على «أنظمة التَّعرُّف على المشاعر» وفقاً للتعريف الذي تضمّنه القانون لهذه الأنظمة

ويعني هذا أن الأنظمة غير الحيوية للتَّعرُّف على المشاعر؛ (مثل الأنظمة النصية) لا تخضع للحظر المنصوص عليه في المادة (٥)، وقد يرجع ذلك إلى عدم دقّة أنظمة التَّعرُّف على المشاعر الحيوية في البيانات التي تفنقر إلى وجود توازن في القوى داخلها؛ مثل بيانات العمل، أو المؤسسات التعليمية^(١٤٧)، ومع ذلك لم يوضّح قانون الذكاء الاصطناعي سبب اعتبار الأنظمة غير الحيوية للتَّعرُّف على المشاعر أقلّ خطراً، أو أكثر دقة من نظيرتها الحيوية

٧- تصنيف البيانات الحيوية^(١٤٨):

يتعلّق هذا الحظر باستخدام أنظمة تصنيف البيانات الحيوية، التي تُصنّف الأفراد؛ بناءً على بياناتهم الحيوية لاستنتاج بعض بيانات الفئات الخاصة بموجب اللائحة العامة لحماية البيانات، والتي تتمثّل في: العرق، الآراء السياسية، العضوية في النقابات العمالية، المعتقدات الدينية أو الفلسفية، الحياة الجنسية، والتوجّه الجنسي

وهناك عدّة بيانات تندرج ضمن الفئات الخاصة لا يشملها هذا الحظر؛ وهي: الأصل العرقي، البيانات الصحية، البيانات الجينية، إلا أنّه من المرجّح تصنيفها – بموجب الملحق الثالث من قانون الذكاء الاصطناعي- على أنها من أنظمة الذكاء الاصطناعي عالية الخطورة

(146) AI Act, Art 3 (39).

(147) AI Act, Recital 44.

(148) AI Act, Art 5 (1) G.

ولا يمل هذا الحظر تصنيف مجموعات البيانات الحيويّة المُكتسبة بشكلٍ قانوني، أو تصنيف البيانات الحيويّة من قِبَل الجهات القائمة على تنفيذ القانون؛ مثل (فرز الصور حسب لون الشعر، أو لون العين من قِبَل الجهات القائمة على تنفيذ القانون للبحث عن المُشتَبِه بهم)

وتجدر الإشارة إلى أنه ليس من اليسير الجزم بما إذا كانت أنظمة التصنيف التي تُستخدم التصنيف الحيوي تندرج ضمن فئة الذكاء الاصطناعي عالي المخاطر؛ حيث تشير الفقرة (٥٤) من القانون إلى أن أنظمة الذكاء الاصطناعي المُخصّصة للتصنيف الحيوي وفقاً للسمات الحساسة، أو بيانات الفئات الخاصّة بموجب اللّائحة العامّة لحماية البيانات - ما لم تكن محظورة بموجب قانون الذكاء الاصطناعي- يجب أن تُصنّف على أنها من الأنظمة عالية المخاطر^(١٤٩).

٨- تحديد الهوية الحيويّة عن بُعد (الآني) في الأماكن العامّة (١٥٠):

يتعلّق هذا الحظر باستخدام أنظمة تحديد الهوية الحيويّة عن بُعد (الآني) (RBI) لأغراض متعلّقة بتنفيذ القانون، وتُعرف هذه الأنظمة بأنها أنظمة ذكاء اصطناعي تُستخدم لتحديد هويّة الأشخاص الطبيعيين دون مشاركتهم، وعادةً ما يتمّ ذلك عن بُعد من خلال مقارنة البيانات الحيويّة بتلك الموجودة بقاعدة بيانات مرجعيّة، كما يشمل هذا الحظر أنظمة الذكاء الاصطناعي التي تتطلب تأخيراً يسيراً في إجراء عمليّة المقارنة؛ إلا أنها تتميز عن أنظمة التحقق حيث لا تعتبر أنظمة التحقق الحيويّة المُستخدمة في (تأكيد هويّة شخص ما للوصول إلى خدمة مُحدّدة، أو الوصول الأمني إلى المباني) من أنظمة الذكاء الاصطناعي التي يشملها الحظر^(١٥١).

وقد تضمّن القانون المذكور عدّة استثناءات، سمح من خلالها للدول الأعضاء باستخدام أنظمة (RBI) لأغراض متعلّقة بتنفيذ القانون في حالات محددة استلزمها الضرورة؛ والتي تتمثل في:

- عمليات البحث التي تستهدف ضحايا جرائم الاختطاف، أو الإتجار بالبشر، أو الاستغلال الجنسي، وكذلك البحث عن الأشخاص المفقودين.
- منع تهديدٍ جوهري، مُحدّد، وشيك لـ (الحياة أو السلامة الجسديّة، تهديد حقيقي؛ حاليّ، أو مُتوقع بهجوم إرهابي).

(149) AI Act, Recital 54.

(150) AI Act, Art 5 (1) H.

(151) AI Act, Recital 15.

• تحديد موقع أو هوية شخص يُشتبه في ارتكابه جريمة؛ وذلك أثناء (إجراء التحقيق الجنائي، المحاكمة، تنفيذ العقوبة) في الجرائم المنصوص عليها في الملحق الثاني؛ مثل الإتجار غير المشروع بالمواد المخدّرة، أو الأعضاء، أو البشر، أو السلاح، بالإضافة إلى جرائم الإرهاب والقتل^(١٥٢).

وبموجب هذه الاستثناءات، يُسمح فقط باستخدام نظام (RBI) لتأكيد هوية الشخص المُستهدف تحديداً، كما يجب أن يُراعى عند استخدام هذا النظام: طبيعة الموقف، «احتمالية، خطورة، حجم» الضرر الذي قد يحدث حال عدم استخدام النظام، كما يجب على الجهات المستخدمة؛ سواء كانت سلطات عامة، أو مؤسسات، أو هيئات، أو مكاتب، أو وكالات تابعة للاتحاد، أو أشخاصاً يتصرفون نيابة عنها؛ تسجيل أنفسهم، واختيار النظام، وتسجيل استخدامه في قاعدة بيانات الاتحاد الأوروبي وفقاً للمادة (٤٩) من القانون^(١٥٣)، والحصول كذلك على إذن مُسبق من سلطة قضائية أو إدارية لكل حالة استخدام (باستثناء الحالات الطارئة)

بالإضافة إلى ذلك، يجب إخطار هيئة مراقبة السوق المختصة، الهيئة الوطنية لحماية البيانات بكل استخدام لنظام (RBI)، كما يجب على السلطة الوطنية في الدولة العضو تقديم تقرير إلى المفوضية الأوروبية التي تُعدّ بدورها تقريراً سنوياً عن حالة استخدام نظام (RBI) وفقاً لهذه الأحكام

سادساً: أنظمة التعرف الحيوي عن بُعد عالية المخاطر:

صنّفت المادة (٦) من قانون الذكاء الاصطناعي بعض أنشطة الذكاء الاصطناعي على أنها «عالية المخاطر»، وقد تضمّن الملحق الثالث قائمة بهذه الأنشطة^(١٥٤)، وقد مُنحت المفوضية الأوروبية صلاحية تعديل هذه القائمة لمواكبة التطورات الحديثة في المجال التكنولوجي^(١٥٥).

وقد تضمّنت هذه القائمة أنظمة التعرف الحيوي عن بُعد (RBI) – التي تُستخدَم في تحديد هوية الأفراد عن بُعد باستخدام البيانات الحيوية – والتي صنّفت كذلك نظراً لحساسية البيانات الحيوية، واتّخذت المادة (٦) من القانون نطاقاً واسعاً شمل – على سبيل المثال – استخدام أنظمة تحديد الهوية الحيوية في الأماكن العامة، من خلال جهات خاصة؛ كمرقبة مداخل الملاعب، أو داخل بعض الأماكن التي لا يُسمح للعامة بالوصول إليها^(١٥٦).

(152) AI Act, Annex II.

(153) AI Act, Art 49.

(154) AI Act, Art 6 (2).

(155) AI Act, Recital 52.

(156) Theodore Christakis, Mathias Becuywe and AI-Regulation Team, Facial Recog-

وتتميّز هذه الأنظمة بأنها تستلزم وقتًا أكبر نسبيًا؛ مقارنةً بـ «أنظمة تحديد الهوية الحيويّة عن بُعد (الآنية) في الأماكن العامّة» بين عمليّة جمع البيانات الحيويّة، ومقارنتها بقاعدة البيانات وانتهاءً بتحديد هويّة أصحابها، وبمعنى آخر لا يُشترطُ لوقوع تلك الأنظمة في نطاق المادة (٦) أن يتمّ تحديد الهوية بشكلٍ فوري، أو أن يُستخدَم النظام لأغراض تتعلّق بتنفيذ القانون^(١٥٧).

ويُستثنى من هذا الحكم، أنظمة التحقّق الحيويّة التي تُستخدَم في تحديد هويّة الشخص^(١٥٨)؛ وهو الأمر الذي يُؤكّد الأهميّة القانونيّة للتمييز بين أنظمة تحديد الهوية، وأنظمة التحقّق من الهوية

وتجدر الإشارة إلى أن قانون الذكاء الاصطناعي يرتّب التزامات عديدة على عاتق مُزوّد ومستخدمي أنظمة الذكاء الاصطناعي عالية المخاطر؛ من بينها: وجوب تطبيق نظام لإدارة المخاطر يتسم بـ (التحليل المستمر للمخاطر المحتملة التي يُشكّلها النظام على الصّحة والسلامة والحقوق الأساسيّة؛ وفقًا للغرض المُستهدف منه، تقدير المخاطر الناشئة عن إساءة الاستخدام المُتوقّعة طوال عمليّة التشغيل، اتخاذ تدابير مناسبة لمعالجة هذه المخاطر)^(١٥٩)؛ بهدف تطوير أنظمة الذكاء الاصطناعي بطريقة تسمح بتقليل المخاطر المحتملة قدر المُستطاع، وكذلك التحكم في المخاطر التي لا يُمكن تفاديها^(١٦٠).

ونظرًا لاستخدام أنظمة التّعريف الحيوي المتطوّرة لنماذج الذكاء الاصطناعي؛ فقد تضمّنت المادة (١٠) من القانون أحكامًا تتعلّق بمعايير جودة البيانات المُستخدمة لتطوير وتدريب هذه الأنظمة، ومن بين عدّة معايير؛ يجب أن تكون هذه البيانات خاليةً من الأخطاء وكاملةً بشكل كافٍ لتحقيق الغرض المقصود منها، كما يجب أن تأخذ مجموعات البيانات في الاعتبار - بالقدر الذي يقتضيه الغرض المقصود من جمعها - السمات أو الخصائص الخاصّة بالبيئة الجغرافيّة، أو السلوكيّة، أو الوظيفة المحدّدة التي يُقصدُ استخدام نظام الذكاء الاصطناعي فيها، كما يجب أيضًا أن يكون الغرض من جمعها شفافًا^(١٦١)، بالإضافة إلى ذلك؛ يجب تصميم نظام الذكاء الاصطناعي لتمكين الرقابة البشريّة من خلال: وضع التصميم المُناسب، تدريب الأفراد المسؤولين عن مراقبة النظام، وبالنسبة لأنظمة (RBI) عالية المخاطر؛ هناك شرطٌ إضافيٌّ يتعلّق بعدم جواز اتّخاذ أيّ قرار؛

inition in the Draft European AI Regulation: Final Report on the High-Level Workshop Held on April 26, 2021 (2021)

(157) Ibid.

(158) AI Act, Annex III 1 (a).

(159) AI Act, Recital 65.

(160) AI Act, Art 9.

(161) AI Act, Recital 67.

باءً على مخرجات النظام وحدها ما لم يتم التحقق منها عن طريق شخصين طبيعيين على الأقل يتمتعان بالكفاءة والتدريب اللازمين، ومع ذلك لا ينطبق هذا الشرط وفقاً للفقرة (٥) من المادة (١٤) – إذا أعلن قانون الاتحاد، أو الدولة العضو عدم تناسب هذا الشرط في المجالات المتعلقة بتنفيذ القانون، أو الهجرة، أو اللجوء، أو مراقبة الحدود.^(١٦٢)

وقد تطلب القانون أيضاً – في المادة (١٥) منه – تطبيق مستويات إلزامية من الدقة والمتانة والأمن السيبراني

بالإضافة إلى ذلك، تخضع أنظمة (RBI) عالية المخاطر لما يُسمّى بـ «تقييم المطابقة» للتحقق من امتثالها لأحكام الفصل الثالث (القسم ٢) من قانون الذكاء الاصطناعي^(١٦٣)، ويُنفَّذ هذا الإجراء في الغالب عن طريق مُقدِّم خدمة الذكاء الاصطناعي ذاته؛ فقد خطط المُشرِّع ترك هذه المسؤولية لهم على الأقل في المرحلة الأولية لتطبيق قانون الذكاء الاصطناعي؛ إلا أنه استثنى أنظمة الذكاء الاصطناعي التي تعتمد على البيانات الحيوية، والتي يجب أن تخضع لتقييم مطابقة من طرف ثالث^(١٦٤)؛ تُجْريه هيئة تقييم المطابقة التي تُعيّنها سلطة «الإخطار» في كل دولة عضو^(١٦٥).

سابعاً: أنظمة التعرف الحيوي محدودة المخاطر:

يمكن تقسيم أنظمة التعرف الحيوي بشكلٍ رئيس إلى نوعين: أنظمة ذكاء اصطناعي محظورة، أنظمة ذكاء اصطناعي عالية المخاطر، ومع ذلك؛ قد يُؤدّي تقييم بعض أنظمة التعرف الحيوي، باعتبارها أنظمة محدودة المخاطر، وقد حدث هذا مع تقنيات التعرف الحيوي المستخدمة في التصنيف الحيوي، والتعرف على المشاعر بموجب الاقتراح الأولي للمفوضية^(١٦٦)؛ إلا أن هذا الوضع ما لبث أن تغير؛ فقد صنف النص النهائي أنظمة التصنيف الحيوي، أنظمة التعرف على المشاعر في الملحق الثالث (١) كأنظمة ذكاء اصطناعي عالية المخاطر^(١٦٧)، ومن ثم؛ فإن أنظمة الذكاء الاصطناعي محدودة المخاطر لا يكون لها ثمة علاقة باستخدام تقنيات التعرف الحيوي في الأماكن العامة.

(162) AI Act, Art 14.

(163) AI Act, Art 43.

(164) AI Act, Recital 125.

(165) AI Act, Art 28.

(166) Recital 70, European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), COM(2021) 206 final.

(167) Artificial Intelligence Act, Annex III(1)(b)–(c) (see also European Parliament, Report on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), A9-0188/2023, where the original wording of Annex III(1)(a) was amended for the first time).

المبحث الرابع مدى كفاية قانون الذكاء الاصطناعي في الحد من المخاطر الناشئة عن استخدام أنظمة التعرف الحيوي

لم ينجُ قانون الذكاء الاصطناعي – منذ طرحه لأول مرة عام ٢٠٢١ – من النقد الموجه إليه من جهات عديدة؛ فبالإضافة إلى المنظمات الدولية التي تعنى بحقوق الإنسان؛ مثل منظمة العفو الدولية^(١٦٨)، تعرّض كذلك للانتقاد من قبل بعض الباحثين؛ لا سيما في مجال أنظمة التعرف الحيوي لأسباب مختلفة؛ من بينها: عدم وضوح المفاهيم، غموض نطاق سريانه، الاستثناءات الواسعة الممنوحة لبعض الأحكام، قصور الحماية المقررة للحقوق الأساسية^(١٦٩).

أولاً: نطاق التطبيق:

سعى قانون الذكاء الاصطناعي إلى تحقيق توازن بين الفوائد التي يحققها الذكاء الاصطناعي؛ بما في ذلك إنفاذ القانون، وحماية الحقوق الأساسية؛ على الأخص الحق في خصوصية البيانات الشخصية، إلا أن نصوص القانون كشفت ميلاً لصالح تحقيق الأمن على حساب الحقوق الأساسية؛ فاستخدام أنظمة التعرف الحيوي لأغراض المراقبة الجماعية يُمكّن السلطات القائمة على تنفيذ القانون من مراقبة أعداد هائلة من الأفراد؛ الأمر الذي يُشكّل تدخلاً خطيراً في الحياة الخاصة لشرائح كبيرة من المجتمع؛ لذلك حظر المشرع هذه الممارسة – في المادة (٥) منه –؛ إلا أنه ما لبث أن وضع عدّة استثناءات سمح من خلالها باستخدام هذه الأنظمة^(١٧٠).

لذا انتقد البعض هذه الاستثناءات، واعتبروها تحايلاً على الحظر المفروض على أنظمة تحديد الهوية الحيوية عند بعد (الأنية) المستخدمة في الأماكن التي يُمكن الوصول إليها بشكل عام؛ حيث سمح القانون – وفقاً لنص المادة (٥) (ح) - باستخدامها لأغراض متعلقة بتنفيذ القانون، وهو ما رأوه توسعاً في الاستثناء من شأنه أن يُفَرِّغ الحظر من كل مضمون^(١٧١).

(168) Amnesty International, 'EU: Artificial Intelligence Rulebook Fails to Stop Proliferation of Abusive Technologies' (Amnesty International, 14 March 2024) <https://www.amnesty.org/en/latest/news/2024/03/eu-artificial-intelligence-rulebook-fails-to-stop-proliferation-of-abusive-technologies/>

(169) Nathalie A Smuha and others, 'How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act' (2021) Social Science Research Network <https://doi.org/10.2139/ssrn.3899991>

(170) AI Act, Recital 32.

(171) ARTICLE 19, 'EU: AI Act Passed in Parliament Fails to Ban Harmful Biometric Technologies' (ARTICLE 19, 13 March 2024) www.article19.org/resources/eu-ai-act-passed-in-parliament-fails-to-ban-harmful-biometric-technologies/

ومع ذلك، تخضع جميع أنظمة تحديد الهوية الحيوية عند بعد (الأنية) المُستخدمة في الأماكن التي يُمكن الوصول إليها بشكل عام المحظورة التي تستخدمها هيئات تنفيذ القانون إلى تقييم يتعلّق بتأثيرها على الحقوق الأساسية، العواقب التي تترتّب على استخدامها، بالإضافة إلى التدابير المُرتبطة بكيفية قُصر التطبيق على ما هو ضروري فيما يتعلّق بالنطاق الجغرافي ومدة الاستخدام^(١٧٢).

وتستند معظم الانتقادات على أنّ قانون الذكاء الاصطناعي، بوضعه الحالي، لا يُشكّل حماية كافية للحقوق الأساسية للأفراد من الطبيعة التدخلية لأنظمة تحديد الهوية الحيوية عن بعد، وخاصةً عند استخدامها للمراقبة الجماعية؛ فالاستثناء المتعلّق باستخدام هذه الأنظمة لتحديد موقع أو هوية شخص يُشتبه في ارتكابه جريمة؛ وذلك أثناء (إجراء التحقيق الجنائي، المحاكمة، تنفيذ العقوبة) في الجرائم المنصوص عليها في الملحق الثاني، الذي تضمّن عدّة جرائم منها: السطو المسلح، الجرائم البيئية، مُجرّد المشاركة في منظمة إجرامية مُتورطة في جريمة، أو أكثر من الجرائم المذكورة، والتي اشترط المشرّع بشأنها - في محاولة منه لتضييق نطاق الاستثناء- أن يكون الحد الأقصى للعقوبة المقررة لأيّ منها لا يقلّ عن ٤ سنوات^(١٧٣)، إلا أنّ هذه المحاولة لم تُفلح في الحدّ من نطاق الاستثناء الذي ظلّ مُتسّعاً، على نحو يُفيد من فعالية الحظر العامّ المفروض على تلك الأنظمة.

كما تعرّض نطاق القانون للانتقاد أيضاً من قِبَل مجالس حماية البيانات الأوروبية (EDPB)، والهيئة الأوروبية لمراقبة حماية البيانات (EDPS) الذين أكّدوا في رأيٍ مُشترك أنّ تحديد الهوية الحيوية للأفراد عن بُعد في الأماكن العامة يحتاج إلى تنظيم أكثر صرامة؛ فالنهج القائم على التمييز بين أنظمة تحديد الهوية الحيوية عند بُعد (الأنية) و (اللاحقة) لا يستند إلى أساس منطقي سليم؛ لأنّ التأثير على الحقوق الأساسية لا يختلف في كلتا الحالتين، كما أنّ التفرقة بين الاستخدام لأغراض تنفيذ القانون والأغراض الأخرى؛ مثل الأمن الخاص تُعدّ تفرقة تحكّمية؛ لأن الطبيعة التدخلية لأنظمة التعرّف الحيوي عند بُعد لا تعتمد بشكل أساسي على الغرض منها؛ لذا اقترح مجلس حماية البيانات الأوروبي، وهيئة حماية البيانات الأوروبية خطراً تاماً لاستخدام أنظمة الذكاء الاصطناعي لغرض التعرّف الآلي على السمات البشرية في الأماكن التي يُمكن الوصول إليها بشكل عامّ تحت أي سياق^(١٧٤)؛

(172) AI Act, Recital 34.

(173) Nathalie A Smuha and others. مرجع سابق.

(174) European Data Protection Board and European Data Protection Supervisor, Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) (18 June 2021) https://www.edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

لا أنه وحتى اليوم لم تشهد المادة (٥) من قانون الذكاء الاصطناعي أي تغييرات (١٧٥)؛ مما يؤكد عدم اعتداد المشرع - إبان وضع الصياغة النهائية للقانون - بهذا النقد

ثانياً: المفاهيم:

أحد أو -ه القصور ذات الأهمية في قانون الذكاء الاصطناعي تلك المتعلقة بتعريف البيانات الحيوية؛ إذ يشير القانون إلى اللأحة العامة لحماية البيانات (GDPR) في حين استلزم هذا المصطلح توضيحاً أكثر تفصيلاً؛ لا سيما فيما يتعلق بتطبيقه على أنظمة التعرف الحيوي المستخدمة في الأماكن العامة؛ بالإضافة إلى ذلك استحدث القانون المذكور عدّة مصطلحات - تضمّنتها المادة (٣) من القانون - منها: «التعرّف الحيوي» (البند ٣٥)، «التحقّق الحيوي» (البند ٣٦)، «نظام تصنيف البيانات الحيوية» (البند ٤٠)، «نظام التعرف الحيوي عن بعد» (البند ٤١)، «نظام التعرف الحيوي عند بعد الآني» (البند ٤٢)، «التعرف الحيوي عند بعد اللاحق» (البند ٤٣)، التي قد تتداخل؛ نتيجة لافتقارها للوضوح من المنظورين العملي والتقني، وهو ما يُعقّد فهم جمهور المستخدمين لهذه المصطلحات، كما أن ميل الجهات العامة القائمة على تنفيذ القانون التي تستخدم تلك الأنظمة نحو السرية مُتذرّعة بأسباب أمنية؛ من شأنه أن يُفاقم المشكلة (١٧٦)؛ فقد يؤدي إلى قيام هذه الجهات بنشر هذه التقنيات دون رقابة كافية على النحو الذي يؤدي إلى تآكل ثقة المجتمع في هذه التقنيات.

كما يعوق غياب التشريعات التي تُقيد بوضوح استخدام الجهات القائمة على تنفيذ القانون لتقنيات الذكاء الاصطناعي (١٧٧) قدرة الأفراد على الحصول على المعلومات، والمطالبة بحقوقهم المتعلقة بهذه البيانات (١٧٨).

(١٧٥) مقارنة نص المادة ٥ (١) ح بين النسخة الأصلية المقترحة من البرلمان الأوروبي والنسخة الحالية من قانون الذكاء الاصطناعي.

(176) P Hacker, 'The Ambivalence of Algorithms: Gauging the Legitimacy of Personalized Law' in M Bakhoun, B Conde Gallego, M-O Mackenrodt and G Surblytè-Namavičienė (eds), *Personal Data in Competition, Consumer Protection and Intellectual Property Law* (Vol 28, Springer 2018) 85 https://doi.org/10.1007/978-3-662-57646-5_5

(177) Theodore Christakis, Mathias Becuywe and AI-Regulation Team, *Facial Recognition in the Draft European AI Regulation: Final Report on the High-Level Workshop Held on April 26, 2021* (AI-Regulation.com 2021) <https://ai-regulation.com/facial-recognition-in-the-draft-european-ai-regulation-final-report-on-the-high-level-workshop-held-on-april-26-2021/>

(178) E Sherwin and E Barysheva, 'Russian Court Rejects Facial Recognition Technology Ban' (DW News, 11 June 2019) <https://www.dw.com/en/russian-court-rejects-call-to-ban-facial-recognition-technology/a-51135814>

بالإضافة إلى ذلك، تسمح القواعد التشريعية المعمول بها للدول الأعضاء بوضع قواعد مختلفة لمعالجة البيانات الحيوية؛ مما يؤدي إلى تضارب في التطبيق؛ نتيجةً للتفسيرات المتباينة التي تنتهجها الدول المختلفة

ومن ناحية أخرى؛ فقد عرف قانون الذكاء الاصطناعي – كما سبق أن ذكرنا- مصطلح «نظام التعرف على المشاعر» على أنه «نظام ذكاء اصطناعي يُستخدَم لغرض تحديد، أو استنتاج مشاعر أو نوايا الأشخاص الطبيعيين؛ بناءً على بياناتهم الحيوية»^(١٧٩)، ووفقاً لهذا التعريف؛ فإنَّ الأنظمة التي تتعرف على المشاعر؛ بناءً على البيانات الحيوية هي التي تُعدُّ فقط من «أنظمة التعرف على المشاعر» على النحو المنصوص عليه في هذا القانون

إلا أنَّ التعرف على المشاعر يُعتبر مجالاً بحثياً مُتعدد التخصصات؛ يشمل: علم النفس، العلوم المعرفية، علوم الحاسب، ويهدف إلى تمكين أجهزة الحاسب من فهم المشاعر، الانفعالات البشرية، والتصرف بناءً عليها^(١٨٠)، حيث يُمكن دمج نظام التعرف على المشاعر في نظام التعرف الآلي على الوجه، الذي يتعرف على الوجه، ويستخرج السمات المطلوبة، ويُصنّف الشخص حسب جنسه وعمره، وستة مشاعر وهيئة أساسية: الغضب، السعادة، الخوف، المفاجأة، الاشمئزاز، الحزن^(١٨١)، كما يُمكن أيضاً أن يشمل التعرف على المشاعر استخدامات لأنواع غير مُصنّفة من البيانات؛ مثل تلك المستمدة من استجابة الجلد (قياس تعرق الجلد لاستنتاج الإثارة العاطفية)، تخطيط كهرباء العضلات (القياس الكهربائي لنشاط العضلات الهيكلية)، قياس التنفّس، ودرجة حرارة الجلد^(١٨٢).

ومع ذلك؛ فإن ما يُعتبر من البيانات الحيوية من الناحية الفنية قد لا يُعدُّ كذلك من الناحية القانونية^(١٨٣)؛ ويرجع ذلك إلى أن تعريف البيانات الحيوية في قانون الذكاء الاصطناعي هو ذات التعريف الذي تضمّنته اللائحة العامة لحماية

(179) AI Act, Art 3 (39).

(180) R W Picard, 'Affective Computing: Challenges' (2003) 59(1) International Journal of Human-Computer Studies 55.

(181) P Lewinski, J Trzaskowski and J Luzak, 'Face and Emotion Recognition on Commercial Property under EU Data Protection Law' (2016) 33(9) Psychology & Marketing 729.

(182) G Udovičić, J Đerek, M Russo and M Sikora, 'Wearable Emotion Recognition System Based on GSR and PPG Signals' in Proceedings of the 2nd International Workshop on Multimedia for Personal Health and Health Care (MMHealth '17) (Association for Computing Machinery, New York, NY, USA, 2017) 53.

(183) C A Jasserand, 'Avoiding Terminological Confusion between the Notions of "Biometrics" and "Biometric Data": An Investigation into the Meanings of the Terms from a European Data Protection and a Scientific Perspective' (2015) 6(1) International Data Privacy Law.

البيانات^(١٨٤)، ويُؤخَذُ على هذا المفهوم أنه مفهوم وظيفي؛ حيث تُحدّد التكنولوجيا المستخدمة لمعالجة البيانات الطبيعة القانونية لهذه البيانات^(١٨٥)، ومن ثمّ لا يُعدّ نظامًا للتعرف على المشاعر ما لم يُعالج بيانات حيويّة؛ الأمر الذي يجعل العديد من أنظمة التعرف على المشاعر خارج نطاق التعريف المُحدّد؛ فالعديد منها لا يعالج بيانات حيويّة وفقًا للتعريف الوارد بقانون الذكاء الاصطناعي لتلك البيانات^(١٨٦).

كما تجدر الإشارة كذلك إلى أنه عادةً ما يتمّ تصنيف استخدام أدوات GPT-أحد تطبيقات "أنظمة الذكاء الاصطناعي للأغراض العامّة"^(١٨٧) - من قبل الهيئات القائمة على تنفيذ القانون بموجب اللائحة العامّة لحماية البيانات (GDPR) على أنها من الأنشطة المحظورة؛ نظرًا لقدرتها على تحليل الصوت والصورة بشكل آني، إلا أن الفقرة (٨٥) من القانون صنفّت هذه الأدوات على أنها أنظمة ذكاء اصطناعي عالية المخاطر قائمة بذاتها، أو جزء من أنظمة ذكاء اصطناعي أخرى عالية المخاطر، وقد أظهرت أمثلة عديدة هذا التضارب؛ فقد فرضت هيئة حماية البيانات الإيطالية حظرًا أوليًا على ChatGPT^(١٨٨)، بينما تساهلت هيئة حماية البيانات النمساويّة تجاه أنشطة «Clearview AI»؛ وهو ما أظهر تباينًا تنظيميًا^(١٨٩) أكّد الحاجة إلى وجود نهج واضح محدد يحمي المصلحة العامّة، ويحمي الحقوق الأساسيّة للأفراد في الوقت ذاته

(184) GDPR, Article 4(14).

(185) E Kindt, 'Having Yes, Using No? About the New Legal Regime for Biometric Data' (2018) 34 *Computer Law & Security Review* 523.

(186) A Kartali, M Roglic, M Barjaktarovic, M Duric-Jovicic and M M Jankovic, 'Real-time Algorithms for Facial Emotion Recognition: A Comparison of Different Approaches' (2018) 14th Symposium on Neural Networks and Applications (NEUREL) 1.

(١٨٧) يُقصدُ به: «نظام ذكاء اصطناعي قائم على نموذج ذكاء اصطناعي للأغراض العامّة، ولديه القدرة على خدمة مجموعة متنوعة من الأغراض؛ سواء للاستخدام المباشر أو للتكامل مع أنظمة ذكاء اصطناعي أخرى». وتُعدّ نماذج الذكاء الاصطناعي للأغراض العامّة مكوّنات أساسية لأنظمة الذكاء الاصطناعي؛ إلا أنها ليست أنظمة ذكاء اصطناعي بحد ذاتها؛ فهناك حاجة إلى عناصر إضافية؛ مثل واجهات المستخدم، لتحويل نماذج الذكاء الاصطناعي للأغراض العامّة إلى أنظمة ذكاء اصطناعي.

AI Act, Art 3 (66), Recital 97.

(188) C Helleputte, S Belotti and F Cieri, 'The Italian DPA Has Its Eyes on Biometric IDs – Another Fight on Tech or a Win for Privacy?' (Privacy World, 9 April 2024) <https://www.privacyworld.blog/2024/04/the-italian-dpa-has-its-eyes-on-biometric-ids-another-fight-on-tech-or-a-win-for-privacy/>

(189) TIPIK Legal, Report on the Implementation of Specific Provisions of Regulation (EU) 2016/679 [Final report] (European Commission Directorate General for Justice and Consumers Unit C.3 Data Protection 2021) <https://www.dataguidance.com/sites/default/files/1609930170392.pdf>

ثالثاً: مبدأ تحديد الغرض:

أكد قانون الذكاء الاصطناعي – في انساق وثيق مع أحكام اللائحة العامة لحماية البيانات (GDPR) - على «مبدأ معالجة البيانات الشخصية لغرض محدد - The principle of purpose limitation- intended purpose»^(١٩٠) – المنصوص عليه في المادة ٣ (١٢) منه، الذي يُعرّف بأنه: «الاستخدام الذي يقصده المزود لنظام الذكاء الاصطناعي؛ بما في ذلك سياق وظروف الاستخدام»؛ وبالتالي فإنَّ أنظمة الذكاء الاصطناعي تكون مُصممة لأغراض مُحددة يحددها «مزود الخدمة»، ويُعتبر من ثمَّ أيُّ انحرافٍ عن الغرض المقصود خرقاً لـ «مبدأ تحديد الأغراض»؛ وهو ما يُعبر عنه قانون الذكاء الاصطناعي بمصطلح «إساءة الاستخدام- reasonably foreseeable misuse» الذي يُعرّف على أنه: «استغلال النظام بطريقة لا تتوافق مع غرضه المقصود، والذي قد ينتج عن سلوكٍ بشريٍّ، أو تفاعل مع أنظمة أخرى؛ بما في ذلك أنظمة الذكاء الاصطناعي الأخرى»^(١٩١).

وقد ألزم القانون «المزود» بإيضاح الغرض المقصود بدقة في الوثائق الفنية، وتعليمات التشغيل الخاصة بالنظام؛ بحيث تتضمن تلك الوثائق ميزات وقدرات النظام وحدوده والبيئة المُخصّصة لاستخدامه^(١٩٢)، كما ألزمه كذلك حال حدوث تعديل جوهري – يعني «تغيير في نظام الذكاء الاصطناعي بعد طرّجه في السوق، أو وضعه في الخدمة؛ والذي لم يكن مُتوقعًا، أو مُخطّطاً له في تقييم المطابقة الأولي، يُؤدّي إلى تعديل الغرض المقصود الذي تمَّ تقييم نظام الذكاء الاصطناعي وفقاً له^(١٩٣) – بأن يخضع لتقييم مطابقة جديد؛ بمعنى أنه عند تعديل استخدام النظام بما يتعارض مع الغرض الأصلي^(١٩٤)، يجب على المزود إعادة تهيئة النظام قانونياً وتقنياً للوفاء بالالتزامات التي يتطلبها القانون؛ خاصةً إذا ترتب على هذا التعديل تغيير في تصنيف النظام؛ بأن أضحى من الأنظمة عالية المخاطر

ونزولاً على ذات المبدأ، أوجب القانون أن تكون البيانات اللازمة للتدريب والتحقّق والاختبار، التي تُستخدَم في الأنظمة عالية المخاطر أن تكون ملائمة، ممثلة بشكل كافٍ، خالية من الأخطاء، وكاملة قدر الإمكان بالنسبة للغرض المقصود^(١٩٥).

(190) AI Act, Art 3 (12).

(191) AI Act, Art 3 (13).

(192) AI Act, Art 3 (12).

(193) AI Act, Art 3 (23).

(194) AI Act, Art 43.

(195) AI Act, Art 10, Recital 67.

وبرغم هذه الضمانات يُواجه تطبيقُ هذا المبدأ على أنظِمة الذكاء الاصطناعي العديد من الصعوبات الناتجة في معظمها عن الطبيعة الخاصّة لهذه الأنظِمة؛ فعلى سبيل المثال تُشكّل أنظِمة الذكاء الاصطناعي مُتعدّدة الأغراض تحديًا كبيرًا لعدم امتلاكها غرضًا ثابتًا محددًا؛ مما يُثيرُ صعوباتٍ حول تصنيفها تحت فئة مُحدّدة من المخاطر؛ فالغرض الرئيس لتلك الأنظِمة لا يتحدّد إلا من خلال معرفة كَيْفِيّة استخدام النظام من قِبَل المستخدم النهائي؛ لذا ذهب بعضُ الباحثين إلى أنّ الغرض المقصود وشروط الاستخدام يجري تحديدها بشكلٍ نهائي من خلال العلاقة التعاقدية بين المُزوّد والمستخدم^(١٩٦).

وفيما يتعلّق بالتعديل الجوهري للغرض المقصود؛ فإنّ الالتزام المفروض على «المُزوّد» بإعادة التقييم – وفقًا للمادة (١٦) - نتيجة تغيير الغرض المقصود، تقتضِ قِيامَ المُزوّد أو طرفٍ ثالث بالإبلاغ عن حدوث هذا التغيير؛ وهو ما قد لا يَحْدُث، ومع ذلك لا توجد آلية تمنع المُزوّد من تحديد غرضٍ مُنّسَع لتقادي تصنيف النظام على أنه من الأنظِمة عالية المخاطر، أو لإتاحة استخدامات مُتعدّدة دون القيام بإعادة التقييم، فضلًا عن ذلك؛ فإنّ الالتزام الخاص بإعادة التقييم يقتصر على الأنظِمة عالية المخاطر؛ ومن ثمّ لا ينطبق إلا على الحالات التي يؤدي فيها تعديل الغرض إلى ارتفاع تصنيف النظام من ناحية المخاطر

بالإضافة إلى ذلك؛ فقد يترتّب على إعادة استخدام البيانات من قِبَل الموزعين – وإن كان مسموحًا قانونًا – خروجًا عن الغرض الأصلي؛ من شأنه أن يُعزّز الأمن العام، وكذلك الحقوق الأساسية للأفراد لمخاطر عديدة؛ ففي دولة المجر - على سبيل المثال - تُستخدَم أنظِمة صور الوجه بشكلٍ أساسي لأغراض تحديد الهوية، وتخضع لتنظيم تشريعي صارم^(١٩٧)، ومع ذلك، قد تُستخدَم ذات البيانات من قِبَل الجهات القائمة على تنفيذ القانون، المصرّح لها قانونًا باستخدام هذه البيانات في مجالاتٍ غير محددة بوضوح^(١٩٨)؛ مما يسمح بالتدخل الوظيفي؛ حيث يتطوّر الغرض المقصود من النظام أثناء التشغيل.

(196) N Helberger and N Diakopoulos, 'ChatGPT and the AI Act' (2023) 12(1) Internet Policy Review <https://doi.org/10.14763/2023.1.1682>

(197) G Gárdonyi, 'Állóképes Arckép Azonosítás Magyarországon [Still Image Face Recognition in Hungary]' (2020) 68(3) *Belügyi Szemle* 22, <https://doi.org/10.38146/BSZ.SPEC.2020.3.2>

(198) Act CCXXII of 2015 (Hungary) <https://njt.hu/jogszabaly/en/2015-222-00-00>

ولتلافي تغيّر الغرض المقصود أثناء تشغيل النظام، وضع قانون الذكاء الاصطناعي عددًا من الآليات لمراقبة تغيّر الغرض؛ منها:

• **نظام المراقبة بعد التسويق (Post-Market Monitoring System):**

ألزم قانون الذكاء الاصطناعي - في المادة (٧٣) منه ^(١٩٩) - «مُزوّد النظام» بإنشاء نظام لرصد الأداء، والامتثال بعد النشر، ويهدف هذا النظام إلى جمع وتحليل البيانات المتعلقة بأداء الأنظمة طوال دورة حياتها؛ لضمان استمرار الامتثال للالتزامات المحددة في الفصل الثالث (القسم الثاني من القانون).

• **تقييم المطابقة (Conformity assessment):** أخضع قانون الذكاء

الاصطناعي - وفقًا لنص المادة (٤٣) منه ^(٢٠٠) - أنظمة الذكاء الاصطناعي عالية المخاطر، التي خضعت بالفعل لإجراء تقييم مطابقة سابق، لإجراء تقييم مطابقة جديد حال إجراء تعديل جوهري.

وفي ذات الشأن، حظّر قانون الذكاء الاصطناعي صراحةً أنظمة تحديد الهوية الحيوية عن بعد (الأنية)، مع بعض الاستثناءات نصّت عليها المادة ٥ (١) (هـ)، وفي المسودة البرلمانية لقانون الذكاء الاصطناعي ^(٢٠١) دعا البرلمان الأوروبي إلى توسيع نطاق الحظر؛ ليشمل أنظمة تحديد الهوية الحيوية (اللاحقة)؛ حيث اقترح التعديل إضافة بند إضافي للمادة ٥ (١) يُحظرُ بموجبه استخدام أنظمة تحديد الهوية الحيوية عن بعد (اللاحقة) في الأماكن التي يُمكن الوصول إليها بشكل عام؛ إلا عن طريق الحصول على إذن قضائي مُسبق للقيام بعمليات بحث ترتبط بمجموعة من الجرائم المُحددة - على النحو المنصوص عليه في المادة ٨٣ (١) من معاهدة عمل الاتحاد الأوروبي TFEU - ، وكان من المحتمل أن يُشكّل هذا المقترح عائقًا أمام تطبيق أنظمة تحديد الهوية الحيوية عن بعد (اللاحقة)؛ إلا أنه لم يُعتمد في النص النهائي الذي أبقى على الحظر المفروض على أنظمة تحديد الهوية الحيوية عن بعد (الأنية)؛ وبالتالي فقد صُنّفت هذه الأنظمة في النسخة النهائية كأنظمة ذكاء اصطناعي عالية المخاطر مع وجود استثناءات واسعة لتطبيقها، بالإضافة إلى تحوّل الإذن القضائي إلى ترخيص إداري؛

(199) AI Act, Art 73.

(200) AI Act, Art 43.

(201) European Parliament, Amendments Adopted by the European Parliament on 14 June 2023 on the Proposal for a Regulation of the European Parliament and of the Council on Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (2023) https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html

ما يُثيرُ مخاوفَ جدِّية بشأن ضعف الرقابة القضائية، وإمكانية إعادة استخدام البيانات على نطاقٍ واسع من قبل الجهات القائمة على تنفيذ القانون

وفي ذات السياق، تجدر الإشارة إلى أنَّه من الضروري الإقرار بأن أي وسيلة من وسائل تحديد الهوية، سواء أُجريت عن بُعد، أو في ذات الموقع، بشكلٍ غير مُتزامنٍ أو آني، قد تُسبب تداخلاً وظيفياً، ومراقبة شاملة إذا تمَّ تعزيزُ النظام بالبيانات المُجمَّعة؛ فالتهديدات لا تتضاءل لمجرَّد منح السلطات أو الشركات وقتاً إضافياً لفحص اللقطات (٢٠٢)؛ لذا فإن تحديد الغرض ووضوحه يُعدُّ عاملاً حاسماً في تقييد ممارسات الرقابة الشاملة التي يُحتملُ أن تقوم بها الجهات القائمة على تنفيذ القانون

وفي ذات الشأن، طُرِحَ بعضُ التساؤلات حول قدرة الهيئات القائمة على تنفيذ القانون على دمج تقنيات التَّعرُّف الحيوي في بنية المراقبة الخاصَّة بها؛ فلم يحظُر التشريع استخدام أنظِمة التَّعرُّف الحيوي عن بعد (الآنية) حظراً تاماً؛ لذا من المُرجَّح أن تقوم هذه الجهات بتركيب التقنيات اللازمة لتطبيق هذه الممارسات على نطاقٍ واسع؛ تحسباً لاستخدامات استثنائية محتملة؛ مما يزيد من خطورة توسُّع نطاق تشغيل هذه التقنيات للحدِّ الذي يتجاوز به الاستثناء المصرَّح به قانوناً؛ إذ لا يُمكنُ للأفراد التحقق من تشغيل النظام إبان تعرضهم له (٢٠٣).

وبناءً على ما تقدَّم؛ يُمكنُ القول إنَّ قانون الذكاء الاصطناعي في صيغته الحاليَّة لا يُناقِش بشكل كافٍ مبدأ تحديد الغرض في سياق أنظِمة الذكاء الاصطناعي لعدَّة أسبابٍ منها:

أ- يركِّز القانون الحالي على بيانات التدريب والإجراءات الفنيَّة المُرتبطة بها، في حين يتجاهل ما يُمكنُ أن يحدثَ فعلاً من إعادة استخدام النماذج المُدرَّبة مُسبِّقاً لتحقيق أغراض ثانويَّة؛ لذا اقترح بعض الباحثين إدراج «مبدأ تحديد الغرض» للنماذج ذاتها؛ بحيث تُصنَّف النماذج بحسب الغرض المُخصَّص لها إبان تدريبها، ويقيد استعمالها بما يتماشى مع ذلك الغرض (٢٠٤).

(202) E Jakubowska, Remote Biometric Identification: A Technical & Legal Guide [Guidance] (European Digital Rights 2023) <https://edri.org/our-work/remote-biometric-identification-a-technical-legal-guide/>

(203) Nathalie A Smuha and others. مرجع سابق.

(204) Rainer Mühlhoff and Hannah Ruschemeier, 'Updating Purpose Limitation for AI: A Normative Approach from Law and Philosophy' (22 January 2024) SSRN <https://ssrn.com/abstract=4711621> or <http://dx.doi.org/10.2139/ssrn.4711621>

ب- الفرض الخاص بقيام المستخدمين بتحديد الغرض الرئيس للنظام – كما هو الحال في أنظمة الذكاء الاصطناعي مُتعددة الأغراض- تخلق حالة من عدم اليقين القانوني؛ لذا اقترح بعض الباحثين تعزيز دور التعليمات التعاقدية؛ لضمان عدم خروج النظم عن الغرض المقصود^(٢٠٥).

وأخيراً، ينبغي الإشارة إلى أن الأحكام التي تضمنها قانون الذكاء الاصطناعي تشكل الحد الأدنى من التنظيم؛ مما يسمح للدول الأعضاء بتطبيق ضمانات أكثر صرامة لحماية الخصوصية، والحقوق الأساسية^(٢٠٦).

رابعاً: مبدأ دقة البيانات:

يربط قانون الذكاء الاصطناعي بشكل سلس بين دقة البيانات، ودقة النظام في سياق تنفيذ القانون، وقد نصت المادة (١٠) من القانون على متطلبات صريحة لجودة البيانات؛ إذ توجب المادة أن تكون البيانات اللازمة للتدريب والتحقق والاختبار، التي تُستخدم في الأنظمة عالية المخاطر أن تكون ملائمة، ممثلة بشكل كافٍ، خالية من الأخطاء وكاملة قدر الإمكان بالنسبة للغرض المقصود^(٢٠٧)، كما استلزمت أيضاً خضوع البيانات لممارسات حوكمة، وضبط ملائمة؛ مثل (توثيق تصميمها، عمليات التنظيم والتصنيف والتحديث والتجميع، التدابير المناسبة للكشف عن التحيزات، ومنعها ومحاولة تلافيتها)، وبموجب هذه الأحكام تلتزم الشركات بتأمين بيانات تدريب عالية الجودة تتسم بالدقة، تراعي التنوع والسياق المتوقع للتطبيق، إضافة إلى إمكانية استخدام بيانات تُصنف على أنها بيانات حساسة؛ بهدف كشف التحيزات وتصحيحها؛ بشرط مراعاة الضمانات المناسبة للحقوق، والحريات الأساسية للأشخاص الطبيعيين^(٢٠٨) بالإضافة إلى شروط معالجة البيانات الشخصية المنصوص عليها في اللائحة العامة لحماية البيانات

وفيما يتعلق بدقة نتائج وأنظمة الذكاء الاصطناعي ذات المخاطر العالية؛ أكد القانون – في المادة (١٥) منه – على وجوب تصميم هذه الأنظمة؛ بحيث تحقق مستوى مناسباً من الدقة والصلابة السيبرانية، وأداءً منتظماً طوال دورة حياتها^(٢٠٩)، كما ألزم البند الثالث من ذات المادة على المُزوّد بالإعلان عن مستويات الدقة،

، مرجع سابق. N Helberger and N Diakopoulos (205)

Phillip Hacker, 'Comments on the Final Trilogue Version of the AI Act' (European New School, 23 January 2024) <https://www.europeannewschool.eu/images/chairs/hacker/Comments%20on%20the%20AI%20Act.pdf> (206)

AI Act, Art 10, Recital 67. (207)

AI Act, Art 10 (5). (208)

AI Act, Art 15. (209)

والمؤشرات المعيارية في تعليمات الاستخدام المُرفقة مع النظام^(٢١٠)، ومن ناحية أخرى؛ يُشجّع القانون المفوضية على التعاون مع جهات مُختصة للقيام بذلك؛ مثل هيئة المقاييس، والمعايير لدراسة أداء الأنظمة^(٢١١).

وقد أضاف القانون العديد من التدابير التي تُسهم في التحقق من دقة مُخرجات الأنظمة في المرحلة اللاحقة لنشر النظام؛ تتمثل في:

• **الاحتفاظ بسجلات التشغيل:** تُوجب المادة (١٢) من القانون على الأنظمة عالية المخاطر الاحتفاظ بتسجيلات تلقائية (logs) لأحداث التشغيل طوال دورة حياة النظام، وفي الحالات الأكثر خطورة، تُوجب تسجيل بياناتٍ تفصيلية؛ مثل قاعدة البيانات المرجعية - قاعدة البيانات التي يتم فحص بيانات الإدخال عن طريقها بواسطة النظام - والنماذج المرجعية المُستخدمة، والبيانات المُدخلة التي تمت معالجتها؛ ومن ثم تُتيح هذه السجلات التتبع الدقيق للقرارات والنتائج؛ فعلى سبيل المثال، يتم تسجيل البيانات التي جرى فحصها مقارنة بالبيانات المُدخلة، وكذلك البيانات التي أدت إلى وجود مطابقة؛ مما يُسهّل تدقيق مخرجات النظام، والتحقق من صحة القرارات المُتخذة.

• **الإشراف البشري:** أوجب القانون تصميم أنظمة الذكاء الاصطناعي عالية المخاطر بطريقة تُمكن الأشخاص الطبيعيين من الإشراف على أدائها، وضمان استخدامها؛ لتحقيق الغرض المنشود، ومعالجة أثارها على مدار دورة حياة النظام^(٢١٢)، ولتحقيق هذه الغاية؛ ينبغي لمُزوّد النظام تحديد تدابير الرقابة البشرية المناسبة قبل طرحه، أو تشغيله داخل السوق؛ ومن بينها:

أولاً: خضوع النظام لقيود تشغيلية مدمجة لا يمكن للنظام تجاوزها.

ثانياً: ضمان استجابة النظام للمشغل البشري.

(210) AI Act, Art 15 (3).

(211) AI Act, Art 15 (2).

(212) AI Act, Art 14.

ثالثاً: أن يتمتع الأشخاص الطبيعيون الذين كُلفوا بالرقابة البشرية بالكفاءة والتدريب، والسلطة اللازمة للاضطلاع بهذا الدور^(٢١٣)، ويكون لهم حسب الظروف:

١- فهم القدرات والقيود المتصلة بالنظام عالي المخاطر فهماً صحيحاً، والقدرة على مراقبة تشغيله على النحو المطلوب؛ بهدف اكتشاف ومعالجة الاختلالات والأداء غير المتوقع.

٢- البقاء على دراية بالميل المُحتمل للاعتماد التلقائي على المُخرجات التي يُنتجها نظام الذكاء الاصطناعي عالي المخاطر، وخاصّةً بالنسبة لأنظمة الذكاء الاصطناعي عالية المخاطر المُستخدَمة لتوفير معلومات، أو توصيات للقرارات التي يجب على الأشخاص الطبيعيين اتّخاذها.

٣- تفسير مُخرَج نظام الذكاء الاصطناعي عالي المخاطر بشكلٍ صحيح، مع مراعاة أدوات وطرق التفسير المُتاحة.

٤- اتّخاذ قرار، في أي حالة معيّنة، بعدم استخدام نظام الذكاء الاصطناعي عالي الخطورة، أو تجاوز أو عكس مخرجات النظام.

٥- التّدخل في تشغيل نظام الذكاء الاصطناعي عالي الخطورة، أو مقاطعة النظام من خلال زر "إيقاف"، أو أي إجراء مُماثل يسمح للنظام بالتوقّف في حالة أمانة.

• **مسئوليّة المزود:** ألزم القانون مُزوّد أنظمة الذكاء الاصطناعي عالية المخاطر بضمان امتثال منتجاتهم لجميع متطلبات القسم الثاني من القانون^(٢١٤)؛ بما في ذلك ضمان دقة وجودة البيانات، ومن ثمّ يتحمّل «المزود» مسئولية مواصفات الدقة من خلال نظام إدارة جودة -؛ وفقاً لما نصّت عليه المادّة (١٧) من القانون-، كما يتحمّل المسئوليّة القانونيّة الناجمة عن الحوادث الناتجة عن عدم دقة البيانات، أو المُخرجات.

(213) AI Act, Recital 73.

(214) AI Act, Art 16.

إلا أنه، وبرغم وجود هذا الإطار القانوني المتشعب؛ فإن بعض المعايير التي تضمنها القانون لدقة البيانات تظل غرضة للتفسير لغموض مضمونها؛ فقد تضمنت المادة (١٠) من القانون مصطلحات؛ مثل «خُلُو البيانات من الأخطاء» في حين لم تضع ذات المادة آلية عملية لضمان تحقيق ذلك، كما لم تضع كذلك تعريفًا واضحًا للتحيز، أو معايير قياسه؛ بما يجعل الالتزام المتعلق بتصحيح التحيز غامضًا^(٢١٥)، بالإضافة إلى خُلُو القانون المذكور من بيان الحد الأدنى لأداء الأنظمة، أو معدلات الخطأ المقبولة، أو إخضاعها لاختبارات تقييم إلزامية؛ لذا يبدو احتمال إنشاء منهجية موحدة على مستوى الاتحاد الأوروبي قائمًا؛ لأن قانون الذكاء الاصطناعي يُشرك المفوضية، بالتعاون مع الجهات الأخرى ذات الصلة، في معالجة الجوانب الفنية لمنهجيات قياس مستويات الدقة المناسبة في المادة ١٥ (٢) من القانون، كما يُحدّد البند (٧٤) دور المفوضية في هذا الأمر؛ مقارنةً بمشاركتها في التوجيهين EU/٣١/٢٠١٤، EU/٣٢/٢٠١٤ بشأن ضمان دقة القياسات، كما يُشير إلى احتمال اتخاذ الاتحاد الأوروبي لإجراءات تنظيمية لضمان دقة أنظمة الذكاء الاصطناعي بما يتماشى مع مبادئ القياس القانونية الأوسع نطاقًا^(٢١٦).

ومن ناحية أخرى؛ فقد ثار تساؤلٌ يتعلّق بكيفية تحديد منهجيات قياس الدقة العامة لتقنية محدّدة، للإجابة على هذا التساؤل؛ ذكر بعض الباحثين أن قواعد الدقة ونظام إدارة الجودة المنصوص عليه في المادة (١٧) من القانون يُقدّم بالفعل إرشاداتٍ حول كيفية موازنة مستويات الدقة مع المبادئ العامة؛ إلا أن المنهجيات العامة لتحديد مستويات الدقة قد لا تتجسّد في تقنية محدّدة بسبب عدّة عوامل^(٢١٧)؛ فمن الناحية الفنية؛ تتفاوت أنظمة القياس الحيوي من حيث مستويات الدقة؛ فنظام التعرف على الوجه - على سبيل المثال - أقلّ دقةً من البيانات الحيوية الأخرى؛ مثل بصمات الأصابع^(٢١٨)، بالإضافة إلى ذلك؛ فإنّ معدلات عدم الدقة في أنظمة التعلم تُعدّ مرتفعة نسبيًا؛ حيث تتغيّر الدقة بمرور الوقت مع إضافة بيانات جديدة، ومن ثمّ؛ فإن المراجعات الدورية لمستويات الدقة المحددة بجانب منهجيتها ضرورية لضمان موثوقية النظام

(215) Sandra Wachter, 'Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond' (2024) 26(3) Yale Journal of Law & Technology <https://ssrn.com/abstract=4924553> or <http://dx.doi.org/10.2139/ssrn.4924553>

(216) AI Act, Recital 74.

(217) G Gültekin-Várkonyi, 'Navigating Data Governance Risks: Facial Recognition in Law Enforcement under EU Legislation' (2024) 13(3) Internet Policy Review <https://doi.org/10.14763/2024.3.1798>

(218) E Garvie, A Bedoya and J Frankle, The Perpetual Line-Up: Unregulated Police Face Recognition in America [Report] (Center on Privacy & Technology at Georgetown Law 2016) <https://www.perpetuallineup.org/risk-framework>

كما تنبغي الإشارة إلى أن قانون الذكاء الاصطناعي يُفْتَقَرُ إلى المرونة والوضوح في هذا الشأن؛ حيث كان ينبغي أن يُشِيرَ إلى أن مستويات الدقة – المُشار إليها في المادة ١٥ (٢) – ليست قياسات ثابتة، بل تُقْبَلُ التعديل وفقاً لفرضيات الاستخدام المختلفة

وقد طُرِحَ تساؤلٌ آخر؛ يتعلّق بكيفية قيام المفوضية الأوروبية - باعتبارها كياناً سياسياً - بالتوصل إلى توافقٍ بشأن منهجيات أدوات قياس دقة أنظمة الذكاء الاصطناعي التي تستخدمها الهيئات القائمة على تنفيذ القانون في الدول الأعضاء؟ تُجَدُّرُ الإشارة إلى أنه حتى الآن، لم تُجرِ مناقشاتٌ حول ذلك الموضوع؛ إلا أنه سيكون من الضروري مشاركة الهيئات القائمة على تنفيذ القانون في هذه المناقشات؛ ممثلةً مصالحها الوطنية؛ لبيان ما إذا كان بإمكانها إيجاد توافقٍ في هذا الشأن

وفي هذا الشأن، اقترح البعض نهجاً محلياً قائماً على تمكين «المزوّد» من تزويد الجهات القائمة على نشر تقنيات القياس الحيوي بتفسيرات مُفصّلة لمستويات الدقة المطلوبة، وإلزام تلك الجهات بتقديم ملاحظاتها؛ لتعزيز شفافية النظام^(٢١٩)، ويجب أن يُراعى في هذا النهج الخبرة الفنية للمزوّد، وإدراكه التام لحالات الاستخدام المُحدّدة لتلافي أيّ أخطارٍ ناشئة عن حالات الاستخدام غير الصحيحة.

وبهدف تلافي المخرجات الخاطئة، يجب استخدام البيانات عالية التمثيل؛ فقد أوضح Fontes وآخرون في تحليلهم لتطبيق Corona الذي يركّز على الخصوصية^(٢٢٠)، والذي فقد التمثيل؛ نتيجة لعدم تمكّنه من جمع بيانات حساسة؛ لذا يجب تغذية الأنظمة ببيانات عالية التمثيل؛ لتجنّب المخرجات غير الصحيحة، وفي سبيل ذلك، يُمكن للسلطات القائمة على تنفيذ القانون، التي تكون على دراية جيدة بالمجموعات التي قد تكون ممثلة تمثيلاً ناقصاً، أن تُقدّم تعليماتها المتعلقة بذلك القصور إلى مُزوّد الخدمة

إضافةً إلى ذلك، اقترح آخرون ترجمة الوثائق التقنية إلى لغة مفهومة، وإنشاء آلية لتلقي الملاحظات من الجمهور حول الإجراءات المُعقّدة؛ فإشراك الجمهور بفاعلية في هذه المناقشات ذات الطابع الحساس يُقلّل الشكوى حول دقة الأنظمة؛ مما يُعزّزُ شرعية استخدامها^(٢٢١).

(219) P Hacker and J-H Passoth, 'Varieties of AI Explanations under the Law. From the GDPR to the AIA, and Beyond' in A Holzinger, R Goebel, R Fong, T Moon, K-R Müller and W Samek (eds), xxAI - Beyond Explainable AI, vol 13200 (Springer 2022) 343 https://doi.org/10.1007/978-3-031-04083-2_17

(220) C Fontes, E Hohma, CC Corrigan and C Lütge, 'AI-powered Public Surveillance Systems: Why We (Might) Need Them and How We Want Them' (2022) 71 Technology in Society 102137 <https://doi.org/10.1016/j.techsoc.2022.102137>

(221) L Urquhart and D Miranda, 'Policing Faces: The Present and Future of Intelli-

خامساً: حقوق صاحب البيانات:

١. الحق في الحصول على المعلومات:

لم يتضمن قانون الذكاء الاصطناعي نصوصاً صريحة تُماثل نصوص المواد ١٢، ١٣، ١٤ من اللائحة العامة لحماية البيانات (GDPR) التي تتعلق بحق الفرد في الحصول على معلومات حول جمع، واستخدام بياناته الشخصية؛ التي من بينها: أغراض معالجة البيانات الشخصية، فترة الاحتفاظ بتلك البيانات، معرفة المصالح المشروعة الخاصة بمراقب البيانات، أو أي شخص آخر حال ما إذا كانت أساساً قانونياً لمعالجة البيانات، الجهات التي سوف تتم مشاركة تلك البيانات معها....، إلا أنه - ومع ذلك - أقر بأن حقوق الأشخاص "أصحاب البيانات" المنصوص عليها في اللائحة العامة لحماية البيانات - فيما يتعلق بهذا التشريع - تظل سارية^(٢٢٢).

كما نصّ على عدّة التزامات تهدف إلى ضمان الشفافية في استخدام أنظمة الذكاء الاصطناعي؛ خاصة تلك التي تُصنّف على أنها «عالية المخاطر»؛ منها على سبيل المثال:

١- ألزمت المادة (١٣) مُزوّدي الأنظمة الذكية عالية المخاطر بتوفير تعليمات واضحة للمستخدمين؛ تشمل معلومات عن قدرات النظام وقيوده والمخاطر المحتملة المرتبطة به.

٢- ألزمت المادة (٥٠) من القانون مُوزّعي أنظمة التّعرف على المشاعر أو أنظمة التصنيف الحيوي بإبلاغ الأشخاص الطبيعيين المُعرّضين لها بتشغيل النظام، ومعالجة البيانات الشخصية ما لم يكن استخدامها في الحالات التي يسمح بها القانون؛ للكشف عن الجرائم الجنائية، أو منعها، أو التحقيق فيها.

٣- ألزم القانون مُوزّعي أنظمة الذكاء الاصطناعي عالية المخاطر المُشار إليها في الملحق الثالث، بإبلاغ الأشخاص الطبيعيين المتأثرين بهذه الأنظمة بخضوعهم لنظام ذكاء اصطناعي^(٢٢٣) على أن يتضمن هذا الإبلاغ: الغرض المقصود، نوع القرارات التي يتم اتّخاذها^(٢٢٤).

gent Facial Surveillance' (2022) 31(2) Information & Communications Technology Law 194 <https://doi.org/10.1080/13600834.2021.1994220>

(222) AI Act, Art 2 (7), Recital 10.

(223) AI Act, Art 26 (11).

(224) AI Act, Recital 93.

ويؤخذُ على هذه النصوص أنها – فيما يتعلّق بالحقّ في الحصول على المعلومات – اقتصرَت على الإحالة إلى اللّائحة العامّة لحماية البيانات، بدلاً من إنشاء آليات مُحدّدة لوضع هذا الحق موضع النفاذ في أنظِمة الذكاء الاصطناعي، كما قصر القانون المذكور التزامات الشفافية على أنظِمة الذكاء الاصطناعي ذات المخاطر العالية، دون باقي الأنظِمة الأقل تصنيفاً؛ والتي تُستخدم بيانات شخصية أيضاً.

لذا؛ نقترح وضع آلية مُحدّدة لتمكين صاحب البيانات من ممارسة هذا الحق، وتحديد الجهة المسؤولة عن الاستجابة لهذا الطلب؛ باعتباره شرطاً لتمكين أصحاب البيانات من ممارسة حقّهم في الاعتراض، أو الطعن على القرارات التي تنتجها أنظِمة الذكاء الاصطناعي

٢. الحقّ في التصحيح:

لم يتضمّن قانون الذكاء الاصطناعي نصّاً صريحاً يُقابِل نصّ المادة (١٦) من اللّائحة العامّة لحماية البيانات التي أقرّت حقّ الشخص صاحب البيانات في تصحيح البيانات غير الدقيقة المتعلّقة به على وجه السرعة، ودون أيّ تأخير غير مُبرّر، كما أقرّت كذلك حقّه في استكمال بياناته المنقوصة، إلا أنّ أحكام اللّائحة العامّة لحماية البيانات – كما سبق أن ذكرنا- تنطبق، جنباً إلى جنب، مع قانون الذكاء الاصطناعي

ومع ذلك؛ فقد أوجب القانون المذكور تصحيح البيانات في حالات مُعيّنة؛ من بينها ما نصّت عليه المادة ١٠ (٥) هـ، التي ألزمت المُزوّد بحذف البيانات الحساسة – التي قام بمعالجتها للضرورة القصوى المتعلّقة باكتشاف التحيُّز ومعالجته - بمجرد تصحيح التحيُّز (٢٢٥)؛ إلا أنه يُعدّ في جوهره التزاماً يقع على عاتق المُزوّد؛ ومن ثمّ لا يُمكنُ اعتباره حقّاً يُمكنُ أن يُطالبَ صاحب البيانات بتطبيقه.

ويؤخذُ على هذا القانون – فيما يتعلّق بالحقّ في التصحيح – أنه:

١- اقتصر على الإحالة إلى اللّائحة العامّة لحماية البيانات، بدلاً من إنشاء آليات مُحدّدة لتنفيذ الحق في التصحيح في سياق أنظِمة الذكاء الاصطناعي؛ مما يترك فجوة في التطبيق العملي لهذا الحق.

٢- تختلف اللائحة العامّة لحماية البيانات عن قانون الذكاء الاصطناعي في تحديد المسؤول؛ فبينما تركز اللائحة على «مراقب البيانات»، يعتمد قانون الذكاء الاصطناعي على «مُزوّد النظام»؛ مما يُؤدّي إلى غموضٍ في تحديد الجهة المسؤولة عن تصحيح البيانات غير الدقيقة.

لذا؛ نقترح إصدار قواعد إرشادية تُوضّح كيفية تنفيذ الحق في التصحيح في سياق أنظمة الذكاء الاصطناعي، مع تحديد المسؤوليات بوضوح؛ لضمان التكامل بين اللائحة العامّة لحماية البيانات، وقانون الذكاء الاصطناعي لتفادي التناقضات، وتسهيل الامتثال لأحكام القانون

٣. الحق في المحو :-

خلا قانون الذكاء الاصطناعي من نصوص تدعم الحق في المحو المنصوص عليه في المادة (١٧) من اللائحة العامّة لحماية البيانات التي تُتيح للأفراد الحق في مسح بياناتهم الشخصية من الجهات التي قامت بجمع تلك المعلومات ومعالجتها، ويُطلَق عليه أيضًا «الحق في النسيان - right to be forgotten»، والذي يُطبّق في حالاتٍ محدّدة، وظروف معيّنة نصّت عليها ذات المادة؛ إلا أن قانون الذكاء الاصطناعي أكّد -كما سبق أن ذكرنا- على أن حقوق الأشخاص «أصحاب البيانات» المنصوص عليها في اللائحة العامّة لحماية البيانات - فيما يتعلّق بهذا التشريع - تظلّ سارية^(٢٢٦).

كما أوجب القانون المذكور حذف البيانات في حالاتٍ مُعيّنة؛ مثل: إلزام المُزوّد بحذف البيانات الحسّاسة - التي قام المُزوّد بمعالجتها للضرورة القصوى المتعلقة باكتشاف التحيز ومعالجته - بمجرد تصحيح التحيز^(٢٢٧)، إلا أن هذا الالتزام لا يرقى إلى اعتباره حقًا يُمكن أن يُطالب صاحب البيانات بتطبيقه

ويواجه تنفيذ الحق في المحو في سياق أنظمة الذكاء الاصطناعي عدّة صعوباتٍ؛ أهمّها:

١- التّحديات التّقنيّة: أنظمة الذكاء الاصطناعي أنظمة مُعقّدة بطبيعتها؛ تعتمد على كمّيّات هائلة من البيانات اللازمة لتدريب النماذج؛ ففي الحالة التي يتمّ فيها تضمين البيانات الشخصية في عمليّة التدريب، يُصبِح من العسير تجنّب وحذف هذه البيانات دون التأثير على أداء النموذج، بالإضافة إلى قيام هذه الأنظمة بطبيعتها باستنتاج بيانات جديدة، مُستخلّصة من البيانات الأصليّة؛ مما يُثير تساؤلاتٍ حول ما إذا كانت هذه البيانات المشتقة تخضع أيضًا لطلبات المحو من عدمه^(٢٢٨).

(226) AI Act, Art 2 (7), Recital 10.

(227) AI Act, Art 10 (5) (e).

(228) Bashirat Bukola, 'Artificial Intelligence and the Right to be Forgotten' (2024) 5(8)

٢- عدم وجود آلية فعّالة لتطبيق الحقّ في المحو: لم يُقدّم قانون الذكاء الاصطناعي آلية فعّالة لتطبيق الحقّ في المحو، على نحوٍ يُجرّد الأفراد من أي وسيلة فعّالة لضمان حذف بياناتهم الشخصية من أنظمة الذكاء الاصطناعي.

٣- عدم وضوح المسؤولية بين الجهات المعنية: لم يُحدّد قانون الذكاء الاصطناعي الجهة المسؤولة عن معالجة البيانات فيما يتعلّق بطلبات محو البيانات.

ولتلافي هذه الصعوبات؛ نقترحُ:

١- إصدار قواعد إرشادية توضح كيفية تنفيذ الحق في المحو في سياق أنظمة الذكاء الاصطناعي، مع تحديد مسؤوليات الجهات المعنية بوضوح؛ لضمان معالجة طلبات المحو بفاعلية.

٢- تطوير تقنيات إزالة التعلّم الآلي «Machine unlearning» التي تهدف إلى إزالة أثر بيانات مُعيّنة من نموذج مُدرّب دون الحاجة لإعادة التدريب الكامل للنظام؛ ومن أمثلة هذه التقنيات: تقنية (ETID (Iterative based-Ensemble Distillation Information التي تهدف إلى تحقيق محو فعّال للبيانات مع الحفاظ على أداء النموذج^(٢٢٩).

٤- الحق في عدم الخضوع لقرارات تُتخذ بطريقة آلية بشكل كامل:

أوجب قانون الذكاء الاصطناعي تطبيقاً لنصّ المادة (١٤) منه – كما ذكرنا في موضع سابق من هذه الدراسة- تصميم أنظمة الذكاء الاصطناعي عالية المخاطر بطريقة تُمكّن الأشخاص الطبيعيين من الإشراف على أدائها، وضمان استخدامها لتحقيق الغرض المنشود، ومعالجة أثارها على مدى دورة حياة النظام؛ إلا أن التنظيم التشريعيّ لهذا الحق يُواجه قصوراً في عدّة أوجه تتمثّل في:

١- غموض مفهوم الإشراف البشري: لم يُحدّد القانون المقصود بـ «الإشراف البشري» على وجه الدقّة، وما إذا كان يُكتفى فيه بالموافقة الشكلية، أم يتطلّب وجود تحليل بشري حقيقي؛ الأمر الذي يترك مجالاً للتفسير ينال من فعالية التنفيذ.

International Journal of Research Publication and Reviews <https://doi.org/10.55248/gengpi.5.0824.2310>

(229) Yuncong Yang and others, 'From Machine Learning to Machine Unlearning: Complying with GDPR's Right to be Forgotten while Maintaining Business Value of Predictive Models' (2024) *arXiv preprint* arXiv:2411.17126 <https://arxiv.org/pdf/2411.17126>

استثناءات واسعة: تضمّن القانون استثناءاتٍ واسعة تُمكّن السلطات من استخدام أنظمة ذكاء اصطناعي عالية المخاطر في أحوال مُعيّنة؛ خاصّةً في مجالات تنفيذ القانون والهجرة ومراقبة الحدود دون الالتزام بمتطلبات الإشراف البشري (٢٣٠).

٢- عدم فعالية الإشراف البشري في بعض الحالات: أظهرت بعض الدراسات أنه قد لا يكون بالفعالية المرجوة دائمًا، خاصّةً في الحالات التي يُواجه فيها المشرفون صعوبةً في تقييم توصيات الأنظمة الذكية (٢٣١).

ولتلافي أوجه القصور التشريعي في تنظيم هذا الحق؛ نقترح:

١- إجراء اختبارات إلزامية لتقييم فعالية الإشراف البشري على أن يتم إدراج متطلبات ذلك الاختبار ضمن نظام إدارة الجودة المنصوص عليه في المادة (١٧) من ذات القانون؛ فإذا تبين من هذه الاختبارات أن الرقابة البشرية لا تمنع الضرر، أو أنها تُقاوم الضرر الحاصل؛ فلا ينبغي الاعتماد عليها؛ لذا ينبغي أن يتضمّن قانون الذكاء الاصطناعي آليةً تحدّ من الرقابة البشرية، أو تحظرها في مثل هذه الحالات (٢٣٢).

٢- توفير التغذية الراجعة للمشرفين البشريين: توفير التغذية الراجعة المستمرة للمشرفين حول قراراتهم السابقة؛ بحيث تُمكنهم من التعرّف على الخوارزمية للتحقق من موثوقية قراراتهم على نحو يُعزّز من فعالية الإشراف البشري (٢٣٣).

٣- تدريب المشرفين البشريين وتأهيلهم: يجب أن يتلقّى الأفراد المسؤولون عن الإشراف البشري تدريباً مناسباً لفهم قدرات وحدود الأنظمة الذكية؛ على أن يشمل هذا التدريب عدّة عناصر؛ أهمها (فهم كيفية عمل نظام الذكاء الاصطناعي وحدوده؛ توقّع متى ينتج النظام نتائج مضلّة أو خاطئة وأسباب ذلك؛ امتلاك مستوى كافٍ من الشك في مخرجات نظام الذكاء الاصطناعي...)؛ بهدف اتّخاذ قرارات مستنيرة؛ بناءً على مخرجات النظام (٢٣٤).

(230) AI Act, Art 14 (5).

(231) Johannes Walter, 'Human Oversight Done Right: The AI Act Should Use Humans to Monitor AI Only When Effective' (2023) ZEW Policy Briefs 02/2023, ZEW – Leibniz Centre for European Economic Research https://www.zew.de/en/publications/human-oversight-done-right-the-ai-act-should-use-humans-to-monitor-ai-only-when-effective-1?utm_source=chatgpt.com#publication532409

(٢٣٢) المرجع السابق.

(٢٣٣) المرجع السابق.

(234) Luke Scanlon, 'What Meaningful Human Oversight of AI Should Look Like' (2022) Pinsent Masons Out-Law <https://www.pinsentmasons.com/out-law/analysis/what-meaningful-human-oversight-of-ai-should-look-like>

١. الحق في الحصول على تفسير للقرارات الفردية:

استحدث قانون الذكاء الاصطناعي – بموجب نصّ المادة (٨٦) منه – الحق في الحصول على تفسير للقرارات الصادرة عن أنظمة الذكاء الاصطناعي، والذي بموجبه يحقُّ لأي شخص يتأثر بقرار صادر عن جهة تستخدم نظام ذكاء اصطناعي عالي المخاطر، منصوص عليه في الملحق الثالث من القانون – باستثناء أنظمة البنية التحتية الحيوية «- Critical infrastructure»، وكان لهذا القرار أثر قانوني، أو تأثير كبير على صحته أو سلامته، أو حقوقه الأساسية، أن يحصل من الجهة المستخدمة للنظام على شرح واضح ومفهوم لدور نظام الذكاء الاصطناعي في عملية اتخاذ القرار والعناصر الرئيسية للقرار المُتخذ^(٢٣٥).

ويتميّز هذا التنظيم بمنح هذا الحق لجميع لأشخاص المتأثرين، والذين يُمكن أن يكونوا من أصحاب البيانات أو من غيرهم، كما يُمكن أن يكونوا من الأشخاص الطبيعيين أو الاعتباريين.

ورغم أهمية هذا الحق؛ إلا أن التنظيم التشريعي لهذا الحق يواجه قصوراً في عدّة أوجه؛ تتمثل في:

١- نطاق التطبيق: يقتصر نطاق الحق في الشرح على القرارات التي تتخذها الجهات المستخدمة لأنظمة ذكاء اصطناعي عالية المخاطر؛ مما يعني أن بعض أنظمة الذكاء الاصطناعي التي قد تؤثر بشكل كبير على الأفراد قد لا تخضع لهذا الحق إذا لم تُصنّف كأنظمة ذكاء اصطناعي عالية المخاطر.

٢- الجهة الملزمة بالشرح: يقع الالتزام بالشرح الوارد بنصّ المادة (٨٦) على عاتق الجهة المستخدمة للنظام دون إلزام «مُزوّد النظام» بالمشاركة في تقديم الشرح؛ الأمر الذي قد يؤدي إلى تقديم شروحات غير دقيقة؛ خاصّة إذا كانت الجهة المستخدمة لا تمتلك فهمًا عميقًا لكيفية عمل النظام^(٢٣٦).

٣- تفسير الأنظمة المُعقّدة: تُثير الأنظمة المُعقّدة التي تُعرَف بالـ «الصناديق السوداء» models box-black صعوبة في تفسير القرارات الناتجة عنها؛ نتيجة للصعوبة

(235) AI Act, Art 86.

(236) Simona Demkova, 'The AI Act's Right to Explanation: A Plea for an Integrated Remedy' (2024) MediaLaws <https://www.medialaws.eu/the-ai-acts-right-to-explanation-a-plea-for-an-integrated-remedy/>

الكامنة في الفهم الحقيقي لآليات عمل هذه الأنظمة، فضلاً عن احتمالية أن يؤدي تفسير واحد إلى نتائج مختلفة، أو أن يكون لنتيجة واحدة تفسيرات متعددة؛ الأمر الذي يثير مخاوف تتعلق بإمكانية التلاعب، على نحو يقوّض فعالية الحق في تحقيق أهدافه المرجوة (٢٣٧).

٤- عدم وجود آلية فعّالة لتطبيق الحق في الشرح: لم يقدم قانون الذكاء الاصطناعي آلية فعّالة لضمان التزام الجهة المستخدمة للنظام بهذا الحق، كما لا توجد آلية للتأكد من أن الشرح المقدم يتلاءم مع متطلبات القانون.

ولتفادي أوجه القصور التشريعي في تنظيم هذا الحق، وضمان تعزيز فعاليته؛ نقترح:

١- نطاق التطبيق: تعديل المادة (٨٦) من القانون؛ ليشمل الحق في الشرح كافة أنظمة الذكاء الاصطناعي التي تؤثر بشكل جوهري على الحقوق الأساسية للأفراد، بغض النظر عن تصنيفها.

٢- الجهة الملزمة بالشرح: تعديل الإطار التشريعي لهذا الحق؛ ليتضمن إلزام المزود بتقديم المعلومات التقنية اللازمة لتفسير القرارات الصادرة عن النظام؛ نظراً لامتلاكه المعرفة الكاملة حول تصميم النظام، وأساليب تدريبه، ومن ثمّ تكون له القدرة على تقديم تفسير سليم فيما يتعلق بالقرارات الناتجة عنه.

٣- اشتراط استخدام نماذج ذكاء اصطناعي قابلة للتفسير «AI Interpretable» (٢٣٨) في بعض الحالات ذات الأهمية.

٢. الحق في الشكوى:

أتاح قانون الذكاء الاصطناعي - وفقاً لنص المادة (٨٥) منه (٢٣٩) - سبيلاً لحماية حقوق الأشخاص الطبيعيين والاعتباريين الذين تتأثر حقوقهم وحرّياتهم سلباً باستخدام أنظمة الذكاء الاصطناعي؛ حيث أجاز لهم تقديم شكوى إلى هيئة مراقبة السوق إذا توافرت لديهم أسباب للاعتقاد بوجود مخالفة لأحكام القانون،

(237) Arno Cuypers, 'The Right to Explanation in the AI Act: A Right to Interpretable Models?' (2024) CiTiP Blog, KU Leuven <https://www.law.kuleuven.be/citip/blog/the-right-to-explanation-in-the-ai-act-a-right-to-interpretable-models/>

(٢٣٨) يُقصدُ بها الأنظمة أو النماذج التي تُقدّم تفسيرات مفهومة للبشر عن كيفية اتّخاذها للقرارات، أو الوصول إلى نتائج معينة.

Tim Miller, 'Explanation in Artificial Intelligence: Insights from the Social Sciences' (2019) 267 Artificial Intelligence 1 <https://www.sciencedirect.com/science/article/pii/S0004370218305988>

(239) AI Act, Art 85.

وُتعالج الشكوى وفقاً للإجراءات والقواعد التي تُضعها هيئة مراقبة السوق في كل دولة عضو^(٢٤٠).

ويختلف تنظيم هذا الحق في قانون الذكاء الاصطناعي عنه في اللائحة العامة لحماية البيانات؛ فبينما أجازت اللائحة العامة لحماية البيانات للشخص صاحب البيانات تقديم شكوى إلى الجهة الرقابية المتواجدة في الدولة العضو التي يقيم بها عادة بشأن أي انتهاك مزعوم إذا اعتقد أن معالجة البيانات الشخصية المتعلقة به تنتهك حقوقه المقررة بموجب اللائحة^(٢٤١)؛ إلا أنه وفي المقابل فقد لا تتعلق الشكوى المُقدّمة بموجب قانون الذكاء الاصطناعي بانتهاك حقوق صاحب الشكوى فحسب، بل بالامتنال لأحكام قانون الذكاء الاصطناعي في المُجمل، بالإضافة إلى ذلك، ووفقاً لأحكام اللائحة العامة لحماية البيانات، لا يجوز تقديم الشكوى إلا من قِبَل أصحاب البيانات؛ في حين أجاز قانون الذكاء الاصطناعي، تقديم الشكوى من أي شخص طبيعي أو اعتباري تتأثر حقوقه وحرّياته سلباً باستخدام أنظمة الذكاء الاصطناعي

إلا أن هذا التنظيم لا يخلو من بعض السلبات التي تتمثل في:

١- عدم وجود إجراءات واضحة لمعالجة الشكاوى: لم تُحدّد المادة (٨٥) من القانون إجراءات مُفصّلة لكيفية تقديم الشكاوى أو معالجتها، كما لم تُحدّد إطاراً زمنياً للرد عليها؛ مما قد يُؤدّي إلى تفاوت في التطبيق بين الدول الأعضاء؛ نتيجة لاختلاف القواعد المُنبّعة في كلّ منها.

٢- قيام نظام الشكوى على الإبلاغ: يعتمد الحق في الشكوى على اكتشاف الشخص الطبيعي أو الاعتباري حدوث انتهاك لأحكام القانون؛ ثم يقوم بإبلاغ السلطة المختصة، إلا أنه - وفي معظم الأحيان - تكون المخالفات خفيفة أو فنية للغاية؛ بحيث يصعبُ على الأفراد العاديين إدراكها؛ مما يُقلّل من فعالية هذا الحق.

٣- عدم وجود آلية للطعن: لم يمنح قانون الذكاء الاصطناعي للشاكي الحق في الطعن على القرار الصادر بناءً على الشكوى؛ خلافاً لللائحة العامة لحماية البيانات التي نصّت صراحةً - وفقاً لنص الفقرة ١٤١(٢٤٢) - على الحق في المراجعة القضائية للقرار الصادر.

(240) AI Act, Art 70.

(241) GDPR, Art.77.

(242) GDPR, Recital 141.

ولمعالجة القصور التشريعي في تنظيم هذا الحق؛ يُمكن:

١- قواعد مُعالجة الشكاوى: يجب إصدار إرشادات مُوحّدة تُحدّد كَيْفِيَّة تقديم الشكاوى ومعالجتها؛ بما في ذلك تحديد الجهة المُختصّة بفحص الشكاوى، الوثائق المطلوبة، الإجراءات المُتّبعة، الإطار الزمني للرد على الشكاوى.

وحتى ذلك الحين يُمكن إجراء التعاون، وتبادل الخبرات بين هيئات مراقبة السوق في الدول الأعضاء عن طريق المجلس الأوروبي للذكاء الاصطناعي «European Artificial Intelligence Board»؛ وذلك للتوافق فيما بينها حول قواعد مُوحّدة لمُعالجة الشكاوى^(٢٤٣).

١- التدقيق الدوري: يعتمد الحق في الشكاوى على الإبلاغ - كما سبق أن ذكرنا - ونظرًا لصعوبة اكتشاف المخالفات؛ لتعلّقها بمسائل فنيّة دقيقة، يجب أن تخضع أنظّمة الذكاء الاصطناعي عالية المخاطر إلى تدقيقٍ دوريٍّ منتظم - دون النظر إلى وجود شكاوى أو عدم وجودها - يشمل (مراجعة الخوارزميّات، مخرجات الأنظّمة)، وهو ما لن يتأتّى إلا من خلال تزويد هيئات مراقبة السوق بأدوات تحليل بياناتٍ ذكيّة يُمكنها تتبّع خوارزميات الأنظّمة بشكلٍ دوري، والتقاط أيّ تغيّر في السلوك أو الغرض.

٢- إيجاد آليّة للطعن: يجب توفير آليّة تتيح لمن تقدّم بشكاوى الطعن على القرار الصادر بشأن شكواه إذا ارتأى صدوره بالمخالفة لأحكام القانون.

سابعًا: تحديد المسؤولية:

أثار استخدام تقنيّات القياس الحيوي في الأماكن العامّة التساؤل عن مدى صعوبة تحديد الشخص، أو الأشخاص المسؤولين عن تشغيل هذه الأنظّمة. الإجابة على هذا التساؤل - على غرار المناقشة المطروحة في إطار اللّائحة العامّة لحماية البيانات - ليست باليسيرة على الجمهور؛ وتكمن هذه الصعوبة في العلاقة التي تربط بين الجهة المُستخدمة للنظام - التي غالبًا ما تكون من الجهات القائمة على إنفاذ القانون- ومُقدّم الخدمة «المزوّد» - الذي يكون في معظم الحالات من الكيانات الخاصّة - التي تسعى غالبًا إلى استغلال التّعثرات لتجنّب المسؤولية القانونيّة، مع الحرص على تعظيم الأرباح؛ لذا ينبغي أن يكون بمقدور الجهات المُستخدمة لهذه الأنظّمة إسنادُ المسؤولية الكاملة، أو الجزئيّة إلى مُزوّد الخدمة

(243) AI Act, Art 65.

إضافةً إلى ذلك؛ فقد أشار قانون الذكاء الاصطناعي – وفقاً لنص المادة ٣ (٤٦) منه – إلى مصطلح «إنفاذ القانون - law enforcement»؛ الذي يعني «الأنشطة التي تقوم بها جهات إنفاذ القانون، أو تلك التي تتصرّف نيابةً عنها لأغراض مُتعدّدة؛ منها: منع الجرائم الجنائية؛ التحقيق فيها؛ الكشف عنها؛ مقاضاة مرتكبيها؛ تنفيذ العقوبات الجنائية؛ الحماية من التهديدات التي تلحق الأمن العام ومنعها، وبناءً على هذا التعريف؛ يُعدُّ من جهات إنفاذ القانون الكيانات الخاصّة، أو الأفراد الذين يتصرّفون نيابةً عن تلك الجهات.

لذا؛ فإنّ غياب الوضوح فيما يتعلّق بالعلاقة بين هذه الكيانات الخارجيّة، وجهات إنفاذ القانون يُثيرُ شكوكاً حول تحديد الجهة التي يجب محاسبتها عن أيّة أخطاءٍ ناتجة عن الاستخدام؛ هل هي جهات إنفاذ القانون، أم مُزوّد الخدمة، أم كلاهما؟ وهذا التعقيد لا يتعلّق فقط بحالات فشل النظام^(٢٤٤)؛ بل يمتدُّ إلى تحديد الجهة التي تُوجّه إليها الشكاوى، أو طلبات التعويض عن الإساءة المحتملة لاستخدام البيانات

علاوةً على ذلك، يُضيف انخراط شركات تعمل تحت مظلة ولاية قضائية مختلفة –؛ مثل أنظمة Clearview AI التي تُشغّلها شركة أمريكية – مستوى آخر من التعقيد؛ حيث يؤدي وجود معايير مُتعدّدة لحماية البيانات بين الولايات القانونية والقضائية المُتعدّدة إلى تضارب تشريعي يعوق الرقابة الفعّالة على هذه التقنيّات؛ بما ينال من الحقوق الأساسيّة لأصحاب البيانات.

ثامناً: حل مُقترح: تعزيز دور تقييم أثر حماية البيانات:

لتعزيز شرعيّة نشر تقنيّات القياس الحيوي؛ يجب على الجهات المُستخدمة لهذه التقنيّات إثبات أن هذه الأنظمة لا تُهدِف إلى تحقيق أهدافها التشغيليّة فحسب؛ بل تسعى أيضاً لتحقيق المصلحة العامّة؛ فقد يكون النهج التصاعدي «من القاعدة إلى القمة» الذي تُكتسبُ من خلاله الجهات القائمة على نشر تقنيّات القياس الحيوي ثقة الجمهور عن طريق مُعالجة مخاوف الخصوصية، وحماية البيانات الشخصية أولاً بشكل أكثر فعاليّة من النهج التشريعي التنزلي

ولتحقيق هذا الهدف؛ يُمكنُ تعزيز دور تقييم أثر حماية البيانات (DPIA)، ودمجه مع نظام إدارة المخاطر الحالي المنصوص عليه في قانون الذكاء الاصطناعي؛

(244) E Moss and J Metcalf, 'The Ethical Dilemma at the Heart of Big Tech Companies' (Harvard Business Review, 14 November 2019) <https://hbr.org/2019/11/the-ethical-dilemma-at-the-heart-of-big-tech-companies>

فقد تضمّن قانون الذكاء الاصطناعي معايير تمثّل الحد الأدنى الذي يجب أن يتوافر لضمان احترام الحقوق الأساسية طوال فترة حياة النظام، والتي تتسبب كثيرًا مع الالتزامات المقررة بموجب اللائحة العامة لحماية البيانات (GDPR)؛ فعلى سبيل المثال يجب أن تخضع أنظمة الذكاء الاصطناعي عالية المخاطر لتقييم أثر الحقوق الأساسية «Assessment Impact Rights Fundamental» (FRIA) – وفقًا لنص المادة (٢٧) من القانون – قبل طرحها في الأسواق، ويُجري المورّع هذا التقييم لقياس مدى تأثير نظام ذكاء اصطناعي مُحدّد على الحقوق الأساسية؛ بدءًا من كميّة، وتوقيت استخدام النظام، الفئات المُحتَمَل تأثرها به، كميّة إشراف البشر عليه، وفي النهاية، يجب على المورّع عرض التدابير الواجب اتّخاذها في حالة تحقّق تلك المخاطر؛ بما في ذلك ترتيبات الحوكمة الداخلية، وآليات تلقي الشكاوى وفحصها

ويشبه هذا التقييم تقييم أثر حماية البيانات «Data protection Impact Assessment» (DPIA) – المنصوص عليه في المادة (٣٥) من اللائحة العامة لحماية البيانات؛ حيث يشترط القانون إجراء تقييم أثر الحقوق الأساسية (FRIA) فقط للجوانب غير المغطاة بتقييم أثر حماية البيانات؛ مما يُنشئ رابطًا بين التقييمين؛ بحيث يُكْمَل كلُّ منهما الآخر

وفي هذه المرحلة يُمكن اعتبار تقييم أثر حماية البيانات جزءًا لا يتجزأ من نظام أوسع لإدارة المخاطر، مع اعتباره آلية محددة ومنفصلة لتقييم البيانات الشخصية التي يُراد مُعالجتها

وَيُمْكِنُ إيجازُ عناصر هذا المقترح في:

١- الاستفادة من الآليات القائمة: يُعْتَبَر دمج تقييم مطور لتأثير حماية البيانات في نظام تقييم أثر الحقوق الأساسية (FRIA) في قانون الذكاء الاصطناعي نهجًا عمليًا؛ لاعتماده على الأطر القانونية القائمة، بدلًا من اشتراط هياكل تنظيمية جديدة مما يُسهّل تطبيقه.

٢- التكامل مع تقييم أثر حماية البيانات: أشرنا – في موضع سابق – أن تقييم أثر حماية البيانات يُركّز بشكل أساسي على معالجة البيانات؛ ومن ثمّ لا يغطي بشكل كامل المخاطر الأوسع نطاقًا؛ مثل المراقبة، التحيز، الدقّة؛ ومن ثمّ يُعدّ تضمين هذا التقييم، ليشمل هذه الجوانب، من شأنه أن يُؤدّي إلى تقييم أكثر شمولًا للمخاطر المحتملة.

٣- إشراك مُزوّدي الأنظمة في إجراء التقييم: يُنفذُ تقييم أثر الحقوق الأساسية (FRIA) في أغلب الأحوال دون إشراك مُزوّدي الأنظمة الذين يُمكنهم تقديم إرشادات فنيّة أساسيّة خاصّة فيما يتعلّق بتحديد فئات الأشخاص الطبيعيين والمجموعات التي يُحتملُ أن تتأثّر باستخدام النظام.

٤- إشراك الجمهور في إجراء التقييم: أكّدت الدراسات المنشورة حول تقييم أثر حماية البيانات على ضرورة مشاركة الجمهور في إجراء هذه التقييمات^(٢٤٥)؛ فكثيراً ما يتمّ إغفال المشاورات العامّة عند صياغة هذه التقييمات، كما تفشل الممارسات القائمة على توعية الجمهور بفعاليتها؛ مُعتمِدةً على مبادرات التوعية العامّة اللاحقة؛ مثل نشر المعلومات على مواقع الشرطة، أو حسابات منصات التواصل الاجتماعي؛ فإذا كان من المقرر إجراء تقييم؛ فيجب إجراؤه قبل معالجة البيانات في نظام الذكاء الاصطناعي، كما يجب أن يتضمّن وصول الجمهور إليه، والتشاور بشأنه قبل معالجتها^(٢٤٦)؛ فإذا لم تُمثّل مصالح الجمهور المتعلّقة، يتعلّق بحماية البيانات أثناء تطوير النظام، ولم تُمنح لهم فرصة المساهمة؛ فقد يُؤدّي ذلك إلى إيجاد تصميم غير مكتمل للنظام يُمكن أن يُؤدّي لاحقاً إلى فشل النظام^(٢٤٧)؛ والذي سيؤثّر على كلّ من مُزوّدي الخدمة، والموزعين؛ ليس فقط من الناحية القانونيّة؛ بل من الناحيتين التقنيّة والعمليّة.

وفي هذا السياق، اقترح بعض الباحثين^(٢٤٨) عدّة طرق يُمكن من خلالها تمكين أصحاب المصلحة (الجمهور) من المشاركة في تقييم أثر حماية البيانات، وفي ضوء نتائج الدراسات المنشورة يتحقّق ذلك من خلال:

١- إشراك أفراد من الجمهور كمراجعين خارجيين؛ لتقييم أثر حماية البيانات، ومن خلال هذه الطريقة يُمكن مراعاة ملاحظات الجمهور في عمليّة صنع القرار اللاحقة.

(245) E Bondi and others, 'Envisioning Communities: A Participatory Approach Towards AI for Social Good' (2021) *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society* 425 <https://doi.org/10.1145/3461702.3462612>

(246) E Moss and others, *Assembling Accountability: Algorithmic Impact Assessment for the Public Interest* (Data & Society 2021) <https://datasociety.net/library/assembling-accountability-algorithmic-impact-assessment-for-the-public-interest/>

(247) T Züger and H Asghari, 'AI for the Public: How Public Interest Theory Shifts the Discourse on AI' (2023) 38 *AI & Society* 815 <https://doi.org/10.1007/s00146-022-01480-5>

(248) M Sloane and others, 'Participation Is Not a Design Fix for Machine Learning' (2022) *Proceedings of the 2nd ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization* 1 <https://doi.org/10.1145/3551624.3555285>

٢- إشراك الأكاديميين والمنظمات غير الربحية في إعداد تقييم أثر حماية البيانات.

تاسعاً: التطورات التكنولوجية المتوقعة

إن التوسع المحتمل لتقنيات القياس الحيوي - نتيجةً للتقدم المستمر في قطاع التكنولوجيا؛ وخاصةً في أداء الحاسب، المُعرّفات الحيوية، الذكاء الاصطناعي - خارج نطاق الجهات العاملة في مجال إنفاذ القانون؛ ليشمل مجالات جديدة؛ مثل الإعلانات والألعاب، وكذلك الرعاية الصحية، والتشخيصات الطبية أمرٌ مثير للاهتمام، ويحمل في طياته آمالاً واعدة؛ فعلى سبيل المثال تمكّن الباحثون من استخدام تقنية التعرف على الوجه «Facial Recognition» (FRT) للكشف المبكر عن بعض الأمراض؛ مثل مرض باركنسون

كما مثل ظهور إمكانيات تكنولوجية جديدة؛ مثل ما يُسمّى بـ«القياسات الحيوية مُتعدّدة الوسائط» التي تُتيح التعرف على الوجه بدقة أكبر توجُّهاً جديراً بالملاحظة في مجال المراقبة العامة^(٢٤٩)؛ حيث تجمع القياسات الحيوية مُتعدّدة الوسائط أكثر من سمة حيوية لتحديد هوية الفرد، وبالتالي تُسهم في تحقيق مستويات عالية من الدقة.

ومن بين التقنيات الواعدة للغاية دمج تقنيتي التعرف على الوجه والأذن؛ نظراً لتميّز الأذن ببنية ثلاثية الأبعاد، تكاد تبقى ثابتة رغم التقدم في السن، واختلاف تعابير الوجه، بالإضافة إلى إمكانية جمع البيانات الحيوية المتعلقة بالوجه والأذن دون الحاجة إلى إجراءات أكثر تدخلية؛ مثل استخدام كاميرات المراقبة التلفزيونية المغلقة؛ ممّا يجعلها فرصة لتعزيز المراقبة المتقدمة^(٢٥٠)؛ الأمر الذي يُؤكّد على التطور المتزايد لتقنيات المراقبة، والحاجة المقابلة إلى ضمانات أقوى

(249) Faslul Haq, Fathima Nasu Sahana and Nadeeka Dissanayake, 'Navigating the Ethical and Technological Landscape: The Future Trajectory of Facial Recognition Technology' (2024) 3 International Journal of Agrobiotechnology and Veterinary Medicine <https://sciencebox.uz/index.php/tibbiyot/article/view/9948/9083>

(250) Yichao Ma, Zengxi Huang, Xiaoming Wang and Kai Huang, 'An Overview of Multimodal Biometrics Using the Face and Ear' (2020) Mathematical Problems in Engineering <https://doi.org/10.1155/2020/6802905>

عاشراً: قانون الذكاء الاصطناعي: هل يُناسب المستقبل؟

تُمثِّل مواكبة التقدم التكنولوجي السريع تحدياً أساسياً لأي تشريع في مجال الذكاء الاصطناعي، وقد حاول القانون التغلب على هذه الإشكالية من خلال إمكانية التعديل السريع لمعظم الملاحق الخاصة بالقانون عن طريق المفوضية الأوروبية؛ كما حاول إيجاد نوع من التوازن بين الأحكام الصارمة والغموض اللازم لإفساح المجال أمام التفسير القضائي لضمان فعالية التطبيق^(٢٥١).

وقد ذهبت لورا كارولي «Laura Caroli» -التي قادت المفاوضات حول الجوانب التقنية لقانون الذكاء الاصطناعي- إلى أن القانون المذكور به عيبٌ وحيدٌ؛ قد يُشكِّل تهديداً خطيراً لفعاليته يتمثّل في اعتماد تصنيف المخاطر على «الاستخدام المقصود»؛ ونظراً لأنّ عدداً قليلاً فقط من الأنظمة يعتمدُ على استخدام واحد فقط؛ الأمر الذي يُؤدّي إلى إمكانية قيام مزودي الأنظمة بالتحايل على القانون عن طريق الادّعاء بأن نظام الذكاء الاصطناعي الخاص بهم غير مُخصَّص لغرض مُدرج في قانون الذكاء الاصطناعي، وهو ما لا يتلاءم مع التقنيات المُعقَّدة والقابلة للتكيف؛ مثل الذكاء الاصطناعي، الأمر الذي يُبرزُ صعوبة مراقبة النشر الفعلي لأنظمة الذكاء الاصطناعي، ومراقبة تطورها بمجرد طرحها داخل السوق^(٢٥٢).

(251) Laura Caroli, 'Will the EU AI Act Work? Lessons Learned from Past Legislative Initiatives, Future Challenges' (International Association of Privacy Professionals, 17 April 2024) <https://iapp.org/news/a/will-the-eu-ai-act-work-lessons-learned-from-past-legislative-initiatives-future-challenges>

(٢٥٢) المرجع السابق.

الخاتمة

نظرًا للتطورات التكنولوجية السريعة في العصر الحالي، وما صاحبها من استخدام لتكنولوجيا الذكاء الاصطناعي في تطوير تقنيات القياس الحيوي لأغراض المراقبة، ومنع التهديدات التي تمس الأمن العام، أتى قانون الذكاء الاصطناعي لمعالجة بعض القضايا الرئيسية في هذا المجال التكنولوجي، الذي - ورغم الانتقادات الواسعة التي واجهها - فقد شكل إطارًا قانونيًا رائدًا عالج مجاليًا واسعًا من الإشكاليات القانونية والأخلاقية التي لم يتم بحثها بصورة مكتملة بعد، وسوف يُظهر التطبيق على المدى الطويل ما إذا كان النهج القائم على المخاطر أساسًا كافيًا لتصنيف أنظمة الذكاء الاصطناعي في ظل الإمكانيات الهائلة لتطبيقاته، وفي هذا السياق، تبرز قدرة المفوضية الأوروبية على تعديل الملحق الثالث من القانون؛ ومن ثم مد نطاق الأحكام التي سنّها التشريع للتطبيق على الأنظمة عالية المخاطر، وسيلة فعالة لمواكبة التطور السريع في قطاع التكنولوجيا

وقد أدى تطبيق تقنيات التعرف الحيوي في الأماكن العامة إلى ظهور العديد من المشاكل المتعلقة بالخصوصية والحقوق الأساسية؛ لذا تدخل القانون؛ فحظر الاستخراج غير المستهدف لصور الوجه من الإنترنت؛ مُجبرًا الشركات على إيجاد أساليب جديدة لإنشاء قواعد البيانات، كما نظم القانون أنظمة التعرف الحيوي عن بُعد (RBI) الأكثر انتهاكًا للحقوق الأساسية، وأطلق عليها (الأنظمة عالية المخاطر)، ولكنه لم يحظرها بالكامل؛ خلافًا لتوصيات مجلس حماية البيانات الأوروبي (EDPB)، وهيئة حماية البيانات الأوروبية (EDPS) الصادرة قبل اعتماد النص التشريعي في صورته النهائية، كما حظر استخدام أنظمة تحديد الهوية الحيوية عن بُعد (الأنية) في الأماكن العامة، إلا أنه وفي الوقت ذاته منح الجهات القائمة على إنفاذ القانون استثناءات واسعة النطاق في هذا الشأن، والتي لن تستطع إجبار هذه الجهات على الامتناع عن هذه الممارسات، مما يحد من فعالية الحظر

ومع ذلك؛ فقد تضمن القانون مبادئ قانونية حاكمية في مجال يعاني - على الأقل جزئيًا - من قصور في التنظيم التشريعي؛ فقد حاول معالجة بعض التحديات المهمة المتعلقة بالتحيز في مجال الذكاء الاصطناعي، والحاجة إلى أنظمة تتسم بالدقة لتطبيق تقنية التعرف الحيوي عن بُعد، وقد أنشأ سبلاً قانونية لحماية حقوق الأفراد وحرّياتهم -؛ سواء كانوا من أصحاب البيانات أو من غيرهم-؛ مثل: الحق في الشكوى، الحق في الحصول على تفسير للقرارات الفردية

علاوةً على ذلك، سعى القانون إلى تقديم تعريفاتٍ شاملةٍ يُمكن أن تُسكِّل مرجعًا لتشريعاتٍ مستقبليةٍ في مجال الذكاء الاصطناعي، ونتيجةً لذلك؛ فإنه من المرجح أن تتأثر به التشريعات المتوقعة صدورها في الولايات القانونية والقضائية المختلفة

وقد توصَّلت الدراسة إلى مجموعةٍ من النتائج؛ أهمُّها:

أولاً: تتعلَّق بيانات القياس الحيوي - كما عرَّفتها اللَّائحة العامَّة لحماية البيانات، وكذلك قانون الذكاء الاصطناعي - بالخصائص الجسدية أو الفسيولوجية أو السلوكية للشخص الطبيعي؛ ولذلك فقد اغتُبِرَت أدوات تعريفٍ فريدة للأشخاص الطبيعيين، ونتيجةً لذلك؛ فقد اسْتُخْدِمَت على نطاقٍ واسعٍ في القطاعين العامِّ والخاصِّ في العديد من المجالات؛ مثل: (تحديد الهوية، إنفاذ القانون: التَّعرُّف على المشتبه بهم، المجال الأمني: التحكم في الدُّخول إلى بعض الأماكن، المجال الصحي: التشخيص الطِّبي لبعض الأمراض، التَّعرُّف على المرضى وإعادة توجيههم، تسهيل عملية القبول للمرضى فاقدِي الوعي، والفئات الخاصة التي تُعاني من صعوباتٍ في التواصل)

ثانياً: تُعدُّ الموافقة كـ «أساس قانوني» لمعالجة البيانات الشخصية - في سياق استخدام تقنيَّات التَّعرُّف الحيوي - معيارًا يَصْغُبُ الامتثال إليه؛ ويرجع ذلك إلى عدَّة أسباب:

١- يجب أن تكون المعلومات المُقدَّمة للشخص موضوع البيانات - امتثالاً للحقِّ في الحصول على المعلومات المنصوص عليه في اللَّائحة العامَّة لحماية البيانات - واضحةً ومُوجزةً؛ مناسبةً لمستوى فهم الفرد المستهدف، وفيما يتعلَّق بتقنيَّات التَّعرُّف الحيوي؛ يجب أن تتضمَّن المعلومات: مواقع تنفيذ التقنية، هويَّة مُستخدمي البيانات، مُدَّة الاحتفاظ بالبيانات، وطريقة الاحتفاظ بها، إجراءات ممارسة الحقوق الممنوحة بموجب اللَّائحة العامَّة لحماية البيانات.

٢- عبء إثبات الموافقة: تقع مسئولية إثبات حصول الموافقة على عاتق «جهات التحكم» في البيانات - وفقاً لنص المادة ٧ (١) من اللَّائحة العامَّة لحماية البيانات - وفي ظل صعوبة إثبات الموافقة الشفوية، يُعدُّ الحصول على موافقة كتابية من كل زائرٍ أمراً في غاية الصعوبة كذلك.

ثالثًا: أدى استخدام أنظمة التعرف الحيوي في الأماكن العامة إلى انتهاك المبادئ الحاكمة لحماية بياناتهم الشخصية؛ ومن أهم هذه المبادئ «مبدأ تقليل البيانات» – المنصوص عليه في المادة (٥) من اللائحة العامة لحماية البيانات -؛ فالنطاق الواسع لأنشطة معالجة البيانات التي تقوم بها الهيئات القائمة على تنفيذ القانون، وقيام بعض الشركات بتطوير خوارزميات تعمل على استخدام بيانات غير ضرورية «مفرطة» — قد يُسبب مخاوف تتعلق بالمراقبة المستمرة؛ حيث تعمل هذه المراقبة الشاملة على تقويض استقلالية الأفراد بشكل كبير، ومن ناحية أخرى، تتطلب بعض أنظمة الذكاء الاصطناعي الاحتفاظ بالبيانات الشخصية لفترات طويلة لأغراض التدريب المستمر، وتحسين الأداء، في الوقت الذي يصعب فيه تحديد ما هو «الحد الأدنى الضروري» من البيانات لتحقيق هدف معين؛ مما قد يؤدي إلى جمع ومعالجة كميات مفرطة من البيانات الشخصية على نحو يتعارض مع مبدأ تقليل البيانات

رابعًا: عملية القياس الحيوي — بحسب طبيعتها وطريقة عملها - مُعرّضة للخطأ في كل مرحلة من المراحل؛ ابتداءً بمرحلة «التسجيل»، ومرورًا بمرحلة «استخراج الميزة»، وانتهاءً بمرحلة «المقارنة»؛ لاعتمادها على عدة عوامل منها: نوع وجودة البيانات التي تم جمعها، عمر التكنولوجيا، عدد القوالب المقدمة للمطابقة، ونتيجة لذلك؛ فقد يتعرض أصحاب البيانات إلى أضرارٍ متعدّدة تتباين في تأثيرها؛ فقد تكون بسيطة؛ مثل تعرّض أصحاب البيانات المؤهلين للرفض بشكلٍ خاطئ؛ مما يؤثّر سلبيًا على حقوقهم؛ كالحق في حرية التنقل (الحق في السفر)، وقد تصل الأضرار إلى التحيز الشديد (التمييز)، وكذلك الاتهام الخاطئ في مجال التحقيقات الجنائية، ومن ناحية أخرى؛ قد يترتب على هذه المعدلات زيادة احتمالية تعرّض النظام للاحتيال.

خامسًا: يتعرض أصحاب البيانات إلى مخاطر ناتجة عن بنية نظام القياس الحيوي؛ من بينها:

- **صعوبة التسجيل:** يواجه العديد من الأنظمة الحيوية صعوبة في تسجيل الخصائص الحيوية لبعض الأفراد، فيمكن لعوامل مثل العمل اليدوي (على سبيل المثال: اهتراء بصمات الأصابع؛ نتيجة الأعمال اليدوية الشاقة)، المناخ والظروف الجوية القاسية — أن تؤدي إلى تدهور البيانات الحيوية؛ فالبيانات ذات الجودة المنخفضة تؤدي إلى زيادة معدلات القبول والرفض الخاطئ.

• **اتخاذ قرارات ذات طابع تمييزي:** فقد أظهرت بعض الدراسات التي تمّ إجراؤها على تقنية التعرف على الوجه، مُعدّلات دقّة أعلى للأفراد ذوي البشرة الفاتحة، والذكور وهو ما أشار إلى وجود تفاوتٍ في الأداء؛ بناءً على النوع، ولون البشرة.

سادسًا: أنظّمة القياس الحيوي، باعتبارها أنظّمة معلومات واتصالات، تكونُ عُرضةً للتّعزّات الأمنية، والهجمات السيبرانية في كافّة مراحل تشغيلها؛ كما هو الحال في أيّ نظامٍ تكنولوجيا معلومات، وتتخذُ هذه المخاطر عدّة صور أهمّها (هجمات أنظّمة التقاط البيانات، الهجمات أثناء عمليّة «استخراج السمات والمقارنة»، الهجمات على وسائط التخزين «مركزيّة أو محليّة»، الهجمات على نظام اتّخاذ القرار، الهجمات أثناء عمليّة نقل البيانات)

سابعًا: أصدر الاتحاد الأوروبي – بتاريخ ٢١ مايو عام ٢٠٢٤ - قانون الذكاء الاصطناعي؛ استهدف من خلاله إنشاء إطارٍ تنظيمي مُنسّق بين الدول الأعضاء في الاتحاد الأوروبي لتطوير الذكاء الاصطناعي، وطرحه في الأسواق، ونشره واستخدامه على نطاقٍ واسع، بالإضافة إلى تشجيع الابتكار في هذا المجال بطريقة تضمّن حماية صحة المواطنين وسلامتهم وحقوقهم الأساسية المنصوص عليها في ميثاق الحقوق الأساسية للاتّحاد الأوروبي

ثامنًا: اتّخذ قانون الذكاء الاصطناعي نطاقًا شخصيًا واسعًا يشملُ ستّ فئاتٍ هم: المُورّدون، والمُورّعون، والمستوردون، ووكلاء التوزيع، ومُصنّعو المنتجات، والممثلون المُفوّضون - واستخدم مصطلح "المُشغّل" لوصفهم جميعًا، كما اتّخذ كذلك نطاقًا إقليميًا واسعًا؛ حيث تنطبق أحكامه عندما يكون نظام الذكاء الاصطناعي، سواءً كان مستقلًا، أو جزءًا من مُنتج: (يُطرحُ أو يُشغّل أو يُستورَد أو يُوزّع داخل الاتحاد الأوروبي؛ يُستخدَم من قبل جهة نشر تتواجد، أو لها مقرٌّ داخل الاتحاد الأوروبي)، كما تنطبق أحكامه كذلك إذا استُخدمت مُخرجات نظام ذكاء اصطناعي خارج الاتحاد الأوروبي في داخل الاتحاد الأوروبي، وفي هذه الحالة، سيخضع مُقدّمو الخدمات والناشرون المتواجدون/المتواجدون خارج الاتحاد الأوروبي أيضًا لنطاق قانون الذكاء الاصطناعي

تاسعًا: انتهج قانون الذكاء الاصطناعي نهجًا واضحًا قائمًا على المخاطر من خلال تكييف الأحكام واجبة التطبيق على أنظّمة الذكاء الاصطناعي، مع نطاق المخاطر المحتملة التي يُشكّلها النظام المعني، لذلك تُصنّف أنظّمة الذكاء الاصطناعي - وفقًا لمخاطرها المُقدّرة مُسبقًا- إلى أربع فئاتٍ؛ هي: (الذكاء الاصطناعي ذو المخاطر غير المقبولة، الذكاء الاصطناعي عالي المخاطر،

الذكاء الاصطناعي منخفض المخاطر، الذكاء الاصطناعي ذو المخاطر الضئيلة)، وتُصنَّفُ أنظُمةُ التَّعرُّفِ الحيوي عن بُعْدٍ، المدعومة بالذكاء الاصطناعي، على أنها أنظُمة ذات مخاطر غير مقبولة، أو عالية المخاطر

عاشراً: أگد قانون الذكاء الاصطناعي - في اتساقٍ وثيقٍ مع أحكام اللأئحة العامة لحماية البيانات (GDPR) - على «مبدأ معالجة البيانات الشخصية لغرضٍ مُحدَّد - The principle of purpose limitation»؛ من خلال مصطلح «الغرض المقصود - intended purpose» - المنصوص عليه في المادة ٣ (١٢) منه؛ وبالتالي فإن أنظُمة الذكاء الاصطناعي تكون مُصمَّمة لأغراضٍ مُحدَّدة يُحدِّدها «مزود الخدمة»، ويُعتَبَر من ثَمَّ أيُّ انحرافٍ عن الغرض المقصود خرقاً لـ «مبدأ تحديد الأغراض»؛ وهو ما يُعَبِّرُ عنه قانون الذكاء الاصطناعي بمصطلح «إساءة الاستخدام - reasonably foreseeable misuse»؛ إلا أن تطبيق هذا المبدأ على أنظُمة الذكاء الاصطناعي يُواجه العديد من الصعوبات الناتجة في معظمها عن الطبيعة الخاصة لهذه الأنظُمة؛ ففي الوقت الذي يتم فيه جمع بيانات القياس الحيوي في البداية لغرضٍ مُحدَّد، يُمكن تدريب خوارزميات الذكاء الاصطناعي لتوليد مُخرجات تُحقِّق أغراضاً أخرى؛ كاستخدام الكاميرات المثبتة في مراكز التسوق لمراقبة الموظفين داخلها، أو تحديد العرق، وهو ما يُعرَفُ باسم التحول الوظيفي، أو التسلسل الوظيفي function creep»»، وقد سمح هذا التحول بمعالجة البيانات الشخصية؛ بما يتجاوز الغرض الأساسي المُستهدف من مُعالجتها؛ كما شكَّلت أنظُمة الذكاء الاصطناعي مُتعدِّدة الأغراض تحدياً كبيراً لعدم امتلاكها غرضاً ثابتاً مُحدَّداً؛ مما يُثيرُ صعوباتٍ حول تصنيفها تحت فئةٍ مُحدَّدة من المخاطر؛ لذا تضمَّن القانون عدَّة آلياتٍ لمراقبة تغيُّر الغرض أثناء تشغيل النظام؛ منها:

• نظام المراقبة بعد التسويق: (Post-Market Monitoring System)

ألزم قانون الذكاء الاصطناعي «مزود النظام» بإنشاء نظامٍ لرصد الأداء، والامتنال بعد النشر، ويهدف هذا النظام إلى جمع وتحليل البيانات المتعلقة بأداء الأنظُمة طوال دورة حياتها لضمان استمرار الامتنال للالتزامات المحددة في الفصل الثالث (القسم الثاني من القانون).

• تقييم المطابقة (Conformity assessment): أخضع قانون الذكاء

الاصطناعي أنظُمة الذكاء الاصطناعي عالية المخاطر التي خضعت بالفعل لإجراء تقييم مطابقة سابق، لإجراء تقييم مطابقةٍ جديد حال إجراء تعديلٍ جوهري.

حادي عشر: ربط قانون الذكاء الاصطناعي بشكلٍ سلس بين دقة البيانات، ودقة النظام في سياق تنفيذ القانون، وقد نصّت المادة (١٠) من القانون على متطلبات صريحة لجودة البيانات؛ إذ تُوجب المادة أن تكون البيانات اللازمة للتدريب والتحقق والاختبار، التي تُستخدَم في الأنظمة عالية المخاطر أن تكون ملائمة، مُمثلة بشكل كافٍ، خالية من الأخطاء وكاملة قَدْرَ الإمكان بالنسبة للغرض المقصود، كما استلزمت أيضاً خضوع البيانات لممارسات حوكمة وضبط ملائمة؛ مثل (توثيق تصميمها، عمليات التنظيم والتصنيف والتحديث والتجميع، التدابير المناسبة للكشف عن التحيزات، ومنعها، ومحاولة تلافيها)، كما أضاف القانون المذكور العديد من التدابير التي تُسهم في التحقق من دقة مخرجات الأنظمة في المرحلة اللاحقة لنشر النظام، تتمثل في: (الاحتفاظ بسجلات التشغيل، الإشراف البشري، مسؤولية المزود عن الأخطاء الناتجة، الحوادث الناتجة عن عدم دقة البيانات أو المخرجات)؛ إلا أن بعض المعايير التي تضمنها القانون لدقة البيانات تظلُّ عرضةً للتفسير؛ لغموض مضمونها، فقد تضمنت المادة (١٠) من القانون مصطلحات؛ مثل «خلو البيانات من الأخطاء»، في حين لم تضع ذات المادة آلية عملية لضمان تحقيق ذلك، كما لم تضع كذلك تعريفاً واضحاً للتحيز، أو معايير قياسه؛ بما يجعل الالتزام المتعلق بتصحيح التحيز غامضاً، كما خلا القانون المذكور من بيان الحد الأدنى لأداء الأنظمة، أو معدلات الخطأ المقبولة، أو إخضاعها لاختبارات تقييم إلزامية

ثاني عشر: لم يتضمن قانون الذكاء الاصطناعي آليات مُحَدَّدة لوضع حقوق أصحاب البيانات موضع النفاذ في سياق أنظمة الذكاء الاصطناعي؛ وذلك رغم إقراره بأن حقوق الأشخاص "أصحاب البيانات" المنصوص عليها في اللائحة العامة لحماية البيانات - فيما يتعلق بهذا التشريع - تظل سارية

ثالث عشر: استحدث قانون الذكاء الاصطناعي سُبُلًا لحماية حقوق الغير ممن تتأثر حقوقهم بقرارات صادرة عن أنظمة الذكاء الاصطناعي؛ تمثلت في: (الحق في الحصول على تفسير للقرارات الفردية، الحق في الشكوى)

رابع عشر: يثير استخدام أنظمة التعرف الحيوي في الأماكن العامة صعوبة في تحديد الشخص، أو الأشخاص المسؤولين عن تشغيل هذه الأنظمة؛ وتكمن هذه الصعوبة في عدم وضوح العلاقة التي تربط بين الجهة المُستخدمة للنظام - التي غالباً ما تكون من الجهات القائمة على إنفاذ القانون- ومُقدِّم الخدمة «المزود» - الذي يكون في معظم الحالات من الكيانات الخاصة -، على نحو يتعدّر معه تحديد الجهة التي يجب محاسبتها عن أية أخطاء ناتجة عن الاستخدام؛ هل هي

جهات إنفاذ القانون، أم مُزوّد الخدمة، أم كلاهما؟ وهذه الصعوبة لا تتعلّق فقط بحالات فشل النظام، بل تمتدّ إلى تحديد الجهة التي تُوجّه إليها الشكاوى أو طلبات التعويض عن الإساءة المحتمّلة لاستخدام البيانات، وتزداد هذه الصعوبة عند اشتراك شركات تعمل تحت مظلة ولايّة قانونيّة وقضائيّة مختلفة؛ الأمر الذي يُؤدّي إلى وجود تضارب تشريعي يعوق الرقابة الفعّالة على هذه الأنظمة لوجود معايير مُتعدّدة لحماية البيانات بين الولايات القانونيّة والقضائيّة المُتعدّدة.

كما خلصت الدراسة إلى العديد من التوصيات؛ أهمّها:

أولاً: نظراً للتحديات القانونيّة والعملية التي تتعلّق بمحاولة تلبية متطلبات الموافقة كأساس قانوني لمعالجة البيانات في سياق أنظمة الذكاء الاصطناعي – المتمثلة في صعوبة الحصول عليها أو إثباتها، على النحو المنصوص عليه في المادّتين 6 (1) (أ)، 9 (2) (أ) من اللائحة العامّة لحماية البيانات؛ لذا يجب استكشاف أسس قانونيّة أخرى لمعالجة البيانات – في سياق هذه الأنظمة – مثل: حماية المصالح الحيويّة للشخص موضوع البيانات ”المادّة 9 (2) (ج)“، المصلحة المشروعة «المادّة 6 (1) (ب)».

ثانياً: لمعالجة المشاكل المتعلقة بـ «مبدأ معالجة البيانات الشخصية لغرض محدد The principle of purpose limitation» في سياق أنظمة الذكاء الاصطناعي، المتمثلة في استخدام نظام الذكاء الاصطناعي لتحقيق غرض آخر خلاف الغرض المقصود من النظام، والتي تُعرّف باسم التحوّل الوظيفي، أو التسلل الوظيفي function creep» نفترح:

• إدراج «مبدأ تحديد الغرض» للنماذج ذاتها؛ بحيث تُصنّف النماذج بحسب الغرض المُخصّص لها إبان تدريبها، ويُقيّد استعمالها بما يتماشى مع ذلك الغرض.

• فيما يتعلّق بأنظمة الذكاء الاصطناعي مُتعدّدة الأغراض: تعزيز دور التعليمات التعاقدية؛ لضمان عدم خروج النظم عن الغرض المقصود.

• تزويد هيئات مراقبة السوق بأدوات تحليل بيانات ذكيّة؛ يُمكنها تتبّع خوارزميات الأنظمة بشكل دوري، والتقاط أيّ تغيير في السلوك أو الغرض.

ثالثاً: نزولاً على مبدأ «دقّة البيانات - The data accuracy principle»، وبالإضافة إلى الالتزامات المنصوص عليها في قانون الذكاء الاصطناعي لضمان مبدأ دقّة البيانات؛ يُمكن تعزيز جودة ودقّة البيانات، وكذا دقّة مخرجات النظام عن طريق اتّخاذ عدة تدابير؛ منها:

- بيان المقصود بمصطلح «خُلُو البيانات من الأخطاء»، ووضع آلية عملية لضمان تحقيق ذلك.
- وضع تعريف واضح لمصطلح «التحيز»، وإيجاد معايير لقياسه.
- ضرورة مشاركة الهيئات القائمة على تنفيذ القانون في المناقشات المتعلقة بالتوصل إلى توافق بشأن منهجيات أدوات قياس دقة أنظمة الذكاء الاصطناعي؛ ممثلة مصالحها الوطنية.
- تبني نهج محلي قائم على تمكين «المزود» من تزويد الجهات القائمة على نشر تقنيات القياس الحيوي بتفسيرات مفصلة لمستويات الدقة المطلوبة، وإلزام تلك الجهات بتقديم ملاحظاتها لتعزيز شفافية النظام.
- يجب تغذية الأنظمة ببيانات عالية التمثيل؛ لتجنب المخرجات غير الصحيحة؛ وفي سبيل ذلك، يُمكن للسلطات القائمة على تنفيذ القانون، التي تكون على دراية جيدة بالمجموعات التي قد تكون ممثلة تمثيلاً ناقصاً، أن تُقدّم تعليماتها المتعلقة بذلك القصور إلى مُزوّد الخدمة.
- ترجمة الوثائق التقنية المتعلقة بالنظام إلى لغة مفهومة، وإنشاء آلية لتلقي الملاحظات من الجمهور حول الإجراءات المُعقّدة.
- تحديث قواعد بيانات المجال التشغيلي للتقنية المستخدمة، وتحسين دقة الخوارزمية.
- وضع معايير فنية تُساعد في تدريب الخوارزمية لتحسين الدقة؛ وتتكوّن هذه المعايير من عدّة عوامل؛ منها: مواصفات الأجهزة، جودة الصور، زاوية التصوير، عمليات إعداد البيانات.

رابعاً: هناك حاجة إلى تبني تعريفات جديدة:

- يجب أن يشمل تعريف البيانات الحيوية – المنصوص عليه في قانون الذكاء الاصطناعي- كافة البيانات الشخصية المتعلقة مباشرة بالخصائص الحيوية، دون تلك التي تُعالج فقط من خلال نظام حيوي؛ فالمعول عليه دوماً في اعتبار البيانات بيانات حيوية؛ هو علاقتها بخصائص معينة للأشخاص الطبيعيين، وليس معالجتها من خلال وسائل تقنية مُحدّدة.

• يتعين إعادة النظر في تعريف نظام "التَّعرُّف على المشاعر"؛ بحيث يُشير إلى القدرة على التَّعرُّف على المشاعر أو العواطف أو استنتاجها؛ دون تحديد كيفية القيام بذلك، فإذا لم تُصنَّف بعض أنظِمة الذكاء الاصطناعي التي تَمثِّلُ هذه القدرة كأنظِمة للتَّعرُّف على المشاعر بموجب التعريف الحالي، فهناك خطرٌ من تسلل العديد من أنظِمة الذكاء الاصطناعي الضارّة عبر قانون الذكاء الاصطناعي ودخول السوق؛ وبالتالي فإنّ التركيز على آثار نظام الذكاء الاصطناعي سيجعل التعريف أكثر مرونة في مواجهة التغيرات التكنولوجيّة.

خامساً: اتخذ قانون الذكاء الاصطناعي – كما سبق أن ذكرنا - نطاقاً إقليمياً واسعاً؛ حيث تنطبق أحكامه في الحالة التي تُستخدَم فيها مُخرجات نظام ذكاء اصطناعي خارج الاتِّحاد الأوروبي في داخل الاتِّحاد الأوروبي؛ ففي هذه الحالة، سيخضع مُقدِّمو الخدمات والناشرون المتواجدون خارج الاتِّحاد الأوروبي أيضاً لنطاق قانون الذكاء الاصطناعي؛ وبالتالي فقد يُشكِّلُ إنفاذ القانون على هذه الأنظِمة تحدياً عملياً؛ الأمر الذي يَسْتَلْزِمُ وجودَ تعاونٍ وتنسيقٍ تشريعي بين الولايات القانونيّة، والقضائيّة المُتعدّدة

سادساً: تُواجه حقوق أصحاب البيانات صعوباتٍ كبيرة عند تطبيقها في سياق أنظِمة الذكاء الاصطناعي؛ وترجع هذه الصعوبات – بشكلٍ رئيس - إلى الطبيعة المُعقَّدة لتلك الأنظِمة؛ لذا سوف نقترح بعض التعديلات التشريعيّة؛ لتمكين أصحاب البيانات من ممارسة حقوقهم بشكلٍ فعّال في سياق هذه الأنظِمة؛ وذلك على النحو التالي:

• **الحق في الحصول على المعلومات:** نقترح وضع آليّة مُحدّدة لتمكين صاحب البيانات من ممارسة هذا الحق، وتحديد الجهة المسؤولة عن الاستجابة لهذا الطلب؛ باعتباره شرطاً لتمكين أصحاب البيانات من ممارسة حقهم في الاعتراض، أو الطعن على القرارات التي تنتجها أنظِمة الذكاء الاصطناعي.

• **الحق في التصحيح:** نقترح إصدار قواعد إرشاديّة تُوضِّح كيفية تنفيذ الحق في التصحيح في سياق أنظِمة الذكاء الاصطناعي، مع تحديد المسؤوليات بوضوح؛ لضمان التكامل بين اللائحة العامّة لحماية البيانات، وقانون الذكاء الاصطناعي؛ لتفادي التناقضات، وتسهيل الامتثال لأحكام القانون.

• الحق في المحو: نقترح:

١- إصدار قواعد إرشادية تُوضِّح كيفية تنفيذ الحق في المحو في سياق أنظمة الذكاء الاصطناعي، مع تحديد مسؤوليات الجهات المعنية بوضوح؛ لضمان معالجة طالبات المحو بفاعلية.

٢- تطوير تقنيات إزالة التعلم الآلي «Machine unlearning» التي تهدف إلى إزالة أثر بيانات معينة من نموذج مُدرَّب دون الحاجة لإعادة التدريب الكامل للنظام؛ ومن أمثلة هذه التقنيات: تقنية (ETID Iterative based-Ensemble Distillation Information).

• الحق في عدم الخضوع لقرارات تتخذ بطريقة آلية بشكل كامل: نقترح:

١- إجراء اختبارات إلزامية لتقييم فعالية الإشراف البشري؛ على أن يتم إدراج متطلبات ذلك الاختبار ضمن نظام إدارة الجودة المنصوص عليه في المادة (١٧) من ذات القانون؛ فإذا تبين من هذه الاختبارات أنَّ الرقابة البشرية لا تمنع الضرر، أو أنها تُفادى الضرر الحاصل؛ فلا ينبغي الاعتماد عليها، لذا ينبغي أن يتضمن قانون الذكاء الاصطناعي آلية تُحدِّد من الرقابة البشرية أو تحظرها في مثل هذه الحالات.

٢- توفير التغذية الراجعة للمشرفين البشريين: توفير التغذية الراجعة المستمرة للمشرفين حول قراراتهم السابقة؛ بحيث تُمكنهم من التعرّف على الخوارزمية للتحقق من موثوقية قراراتهم على نحو يُعزِّز من فعالية الإشراف البشري.

٣- تدريب المشرفين البشريين وتأهيلهم: يجب أن يتلقَّى الأفراد المسؤولون عن الإشراف البشري تدريباً مناسباً؛ لفهم قدرات وحدود الأنظمة الذكية؛ على أن يشمل هذا التدريب عدّة عناصر؛ أهمها (فهم كيفية عمل نظام الذكاء الاصطناعي وحدوده؛ توقُّع متى يُنتج النظام نتائج مُضللة أو خاطئة وأسباب ذلك؛ امتلاك مستوى كافٍ من الشك في مخرجات نظام الذكاء الاصطناعي...)؛ بهدف اتِّخاذ قرارات مستنيرة؛ بناءً على مخرجات النظام.

سابعاً: استحدث قانون الذكاء الاصطناعي – كما سبق أن ذكرنا - سُبلاً لحماية حقوق الغير ممَّن تتأثر حقوقهم بقرارات صادرة عن أنظمة الذكاء الاصطناعي؛ تمثَّلت في: (الحق في الحصول على تفسير للقرارات الفردية، الحق في الشكوى)؛ إلا أنَّ التنظيم التشريعي لهذه الحقوق في قانون الذكاء الاصطناعي يُواجه قصوراً؛ ولتفادي القصور التشريعي في تنظيم هذه الحقوق، وضمان تعزيز فعاليتها نقترح:

• الحق في الحصول على تفسير للقرارات الفردية: نقترح:

- ١- نطاق التطبيق: تعديل المادة (٨٦) من القانون؛ ليشمل الحق في الشرح كافّة أنظمة الذكاء الاصطناعي التي تُؤثّر بشكلٍ جوهري على الحقوق الأساسية للأفراد؛ بغضّ النظر عن تصنيفها.
- ٢- الجهة المُلتزمة بالشرح: تعديل الإطار التشريعي لهذا الحق؛ ليتضمّن إلزام المزود بتقديم المعلومات التقنيّة اللازمة لتفسير القرارات الصادرة عن النظام؛ نظرًا لامتلاكه المعرفة الكاملة حول تصميم النظام، وأساليب تدريبه؛ ومن ثمّ تكون له القدرة على تقديم تفسيرٍ سليم فيما يتعلّق بالقرارات الناتجة عنه.
- ٣- اشتراط استخدام نماذج ذكاء اصطناعي قابلة للتفسير «Interpretable AI» في بعض الحالات ذات الأهميّة.

• الحق في الشكوى: نقترح:

- ١- قواعد مُعالجة الشكاوى: يجب إصدار إرشادات مُوحّدة تُحدّد كيفية تقديم الشكاوى ومعالجتها؛ بما في ذلك: تحديد الجهة المختصة بفحص الشكاوى، الوثائق المطلوبة، الإجراءات المُتبعة، الإطار الزمني للردّ على الشكاوى.
- ١- وحتى ذلك الحين، يُمكن إجراء التعاون، وتبادل الخبرات بين هيئات مراقبة السوق في الدول الأعضاء عن طريق المجلس الأوروبي للذكاء الاصطناعي «European Artificial Intelligence Board»؛ وذلك للتوافق فيما بينها حول قواعد مُوحّدة لمُعالجة الشكاوى.
- ٢- التدقيق الدوري: يعتمد الحق في الشكوى على الإبلاغ - كما سبق أن ذكرنا - ونظرًا لصعوبة اكتشاف المخالفات لتعلّقها بمسائل فنيّة دقيقة؛ لذا يجب أن تخضع أنظمة الذكاء الاصطناعي عالية المخاطر إلى تدقيق دوري منتظم - دون النظر إلى وجود شكوى أو عدم وجودها - يشمل (مراجعة الخوارزميات، مخرجات الأنظمة).
- ٣- إيجاد آليّة للطّعن: يجب توفير آليّة تُتيح لمن تقدّم بشكوى الطعن على القرار الصادر بشأن شكواه إذا ارتأى صُدوره بالمخالفة لأحكام القانون.

ثامناً: نزولاً على مبدأ أمن البيانات «Data Security» -؛ باعتباره أحد المبادئ الأساسيّة لمُعالجة البيانات الشخصية؛ وفقاً للمادة (٥) من اللائحة العامّة لحماية البيانات (GDPR) - والذي يهدف إلى ضمان حماية البيانات الشخصية من الوصول غير المُصرّح به، المُعالجة غير المشروعة، بالإضافة إلى الحماية من الضياع أو التلف؛ سواءً كان عرضياً، أو ناتجاً عن سوء إدارة أو خرقٍ أمني،

ولما كانت أنظمة القياس الحيوي - باعتبارها أنظمة معلومات واتصالات - تُعتبر عُرضةً للتهديدات الأمنية والهجمات السيبرانية في كافة مراحل تشغيلها؛ كما هو الحال في أي نظام تكنولوجي معلومات؛ لذا يُمكن اتخاذ العديد من التدابير الأمنية التي تستهدف تعزيز أمن البيانات في سياق هذه الأنظمة، والتي تختلف باختلاف نوع الخطر الذي تتعرض له؛ وذلك على النحو الآتي:

• **هجمات أنظمة التقاط البيانات:** نظراً لشيوع هجمات انتحال الهوية؛ فقد جرى اقتراح بعض الأساليب للتغلب على تلك الهجمات؛ منها:

١- كشف الهوية الحيوية: استخدام التقنيات للتحقق من أن العينة الحيوية مُستخرجة من شخص حي، وتتخذ هذه الطريقة إحدى صورتين: (الأولى: الكشف الإيجابي عن الهوية الحيوية: الذي يتطلب تفاعلاً من المستخدم كالابتسام مثلاً)، (الثانية: الكشف السلبي عن الهوية الحيوية: يستخدم تحليلاً متقدماً لخصائص معينة؛ مثل: ملمس الجلد، قياس درجة حرارة الجسم، نبض الدم).

٢- اختبار العلاقة بين الشخص والبيانات الملتقطة: بالنسبة إلى أنظمة بصمات الأصابع، قد يصعب استخدام أصابع متعددة (بتسلسل محدد) القدرة على الانتحال.

٣- الإشراف على مواقع جمع البيانات.

٤- تركيب كاميرات في مواقع التقاط البيانات.

٥- استخدام أنظمة قياس حيوي متعددة الوسائط (تستخدم سمات حيوية متعددة).

٦- المصادقة متعددة العوامل: دمج القياسات الحيوية مع طرق المصادقة الأخرى لتعزيز الأمان.

• **الهجمات على وسائط التخزين «مركزية أو محلية»:** للحد من هذه الهجمات؛ يُمكن اتخاذ تدابير أمنية؛ مثل تخزين البيانات في وحدات تخزين مقاومة للعبث، لا تقبل التخزين أكثر من مرة واحدة فقط.

• **الهجمات أثناء عملية نقل البيانات:** للحد من هذا النوع من الهجمات يُمكن تطبيق العديد من الحلول؛ منها: تطبيق تقنيات اتصال آمنة، تشفير المعلومات المُرسلة، تقليل الوصول إلى البنية التحتية المادية، استخدام رموز الجلسة من خلال عملية عشوائية، المراقبة الشاملة للبنية التحتية.

تاسعاً: لتعزيز سرعة نشر تقنيات القياس الحيوي؛ يجب على الجهات المستخدمة لهذه التقنيات إثبات أن هذه الأنظمة تسعى إلى تحقيق المصلحة العامة، على نحو تكتسب معه ثقة الجمهور عن طريق معالجة مخاوف الخصوصية، وحماية البيانات الشخصية

ولتحقيق هذا الهدف؛ يُمكن تعزيز دور تقييم أثر حماية البيانات (DPIA) – المنصوص عليه في اللائحة العامة لحماية البيانات (GDPR) –، ودمجه مع نظام إدارة المخاطر الحالي المنصوص عليه في قانون الذكاء الاصطناعي، حيث يُمكن اعتبار تقييم أثر حماية البيانات جزءاً لا يتجزأ من نظامٍ أوسع لإدارة المخاطر، مع اعتباره آليةً مُحددة ومنفصلة لتقييم البيانات الشخصية التي يُرادُ مُعالجتها

ويُمكن إيجاز عناصر هذا المقترح في:

١- الاستفادة من الآليات القائمة: يُعتبر دمج تقييم مطور لتأثير حماية البيانات في نظام تقييم أثر الحقوق الأساسية (FRIA) في قانون الذكاء الاصطناعي نهجاً عملياً؛ لاعتماده على الأطر القانونية القائمة، بدلاً من اشتراط هياكل تنظيمية جديدة؛ مما يُسهّل تطبيقه.

٢- التكامل مع تقييم أثر حماية البيانات: أشرنا – في موضع سابق – أن تقييم أثر حماية البيانات يُركّز بشكلٍ أساسي على معالجة البيانات؛ ومن ثمّ لا يغطي، بشكلٍ كامل، المخاطر الأوسع نطاقاً؛ مثل المراقبة، التحيز، الدقة؛ ومن ثمّ يُعدّ تضمين هذا التقييم ليشمل هذه الجوانب، من شأنه أن يُؤدّي إلى تقييم أكثر شمولاً للمخاطر المحتملة.

٣- إشراك مزودي الأنظمة في إجراء التقييم: يُنفذ تقييم أثر الحقوق الأساسية (FRIA) في أغلب الأحوال دون إشراكٍ مُزوّدٍ الأنظمة الذين يُمكنهم تقديم إرشادات فنية أساسية؛ خاصةً فيما يتعلّق بتحديد فئات الأشخاص الطبيعيين، والمجموعات التي يُحتمل أن تتأثر باستخدام النظام.

٤- إشراك الجمهور في إجراء التقييم: أكّدت الدراسات المنشورة حول تقييم أثر حماية البيانات على ضرورة مشاركة الجمهور في إجراء هذه التقييمات.

قائمة المراجع

- Els J Kindt, Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis (Springer 2013) 369.
- J Breebaart, B Yang, I Buhan-Dulman and C Busch, 'Biometric Template Protection' (2009) 301.
- P Hacker and J-H Passoth, 'Varieties of AI Explanations under the Law. From the GDPR to the AIA, and Beyond' in A Holzinger, R Goebel, R Fong, T Moon, K-R Müller and W Samek (eds), xxAI - Beyond Explainable AI, vol 13200 (Springer 2022) 343 https://doi.org/10.1007/978-3-031-04083-2_17
- P Hacker, 'The Ambivalence of Algorithms: Gauging the Legitimacy of Personalized Law' in M Bakhoun, B Conde Gallego, M-O Mackenrodt and G Surblytė-Namavičienė (eds), Personal Data in Competition, Consumer Protection and Intellectual Property Law (Vol 28, Springer 2018) 85 https://doi.org/10.1007/978-3-662-57646-5_5
- W Boron and E Boulpaep, Medical Physiology (Elsevier 2008).

• Journal Articles:

- "Use of Facial Recognition Technology for Medical Purposes: Balancing Privacy with Innovation" (2016) 43(4) Pepperdine Law Review 1017, 1022.
- A K Jain, A Ross and S Pankanti, 'A Prototype Hand Geometry-based Verification System', in Proceedings of the Second International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA) (Washington DC, USA, 1999); Joint Research Centre (JRC), Biometrics at the Frontiers (2005) 62.
- Andrea Rosales and Mireia Fernández-Ardèvol, 'Ageism in the Era of Digital Platforms' (2020) Convergence <https://journals.sagepub.com/doi/full/10.1177/1354856520930905>.
- Ayanna Howard and Charles Isbell, 'Diversity in AI: The Invisible Men and Women' (21 September 2020) MIT Sloan Management Review <https://sloan-review.mit.edu/article/diversity-in-ai-the-invisible-men-and-women/>
- Bashirat Bukola, 'Artificial Intelligence and the Right to be Forgotten' (2024) 5(8) *International Journal of Research Publication and Reviews* <https://doi.org/10.55248/gengpi.5.0824.2310>

- Byoungjun Jeon and others, 'A Facial Recognition Mobile App for Patient Safety and Biometric Identification: Design, Development, and Validation' (2019) 7(4) JMIR mHealth and uHealth 1.
- C A Jasserand, 'Avoiding Terminological Confusion between the Notions of "Biometrics" and "Biometric Data": An Investigation into the Meanings of the Terms from a European Data Protection and a Scientific Perspective' (2015) 6(1) International Data Privacy Law.
- C Fontes, E Hohma, CC Corrigan and C Lütge, 'AI-powered Public Surveillance Systems: Why We (Might) Need Them and How We Want Them' (2022) 71 Technology in Society 102137 <https://doi.org/10.1016/j.tech-soc.2022.102137>
- Clive Norris, 'From Personal to Digital: CCTV, the Panopticon, and the Technological Mediation of Suspicion and Social Control' in David Lyon (ed), Surveillance as Social Sorting (Routledge 2002) 249–281 <https://doi.org/10.4324/9780203994887> accessed 31 May 2025.
- David Lyon, 'Surveillance' (2022) 11(4) Internet Policy Review <https://doi.org/10.14763/2022.4.1673> accessed 31 May 2025.
- Dian Hong and others, 'Genetic Syndromes Screening by Facial Recognition Technology: VGG-16 Screening Model Construction and Evaluation' (2021) 16 Orphanet Journal of Rare Diseases 1.
- E Kindt, 'Having Yes, Using No? About the New Legal Regime for Biometric Data' (2018) 34 Computer Law & Security Review 523.
- Erik Snijder, Het biometrisch paspoort in Nederland: crash of zachte landing (2010) 70–72.
- Esefan Ortiz, Kevin W Bowyer and Patrick J Flynn, 'A Linear Regression Analysis of the Effects of Age Related Pupil Dilation Change in Iris Biometrics' (2013) https://www3.nd.edu/~kwb/Ortiz_Bowyer_Flynn_BTAS_2013.pdf accessed 1 June 2025.
- Faslul Haq, Fathima Nasu Sahana and Nadeeka Dissanayake, 'Navigating the Ethical and Technological Landscape: The Future Trajectory of Facial Recognition Technology' (2024) 3 International Journal of Agrobiotechnology and Veterinary Medicine <https://sciencebox.uz/index.php/tibbiyot/article/view/9948/9083>

- G Gárdonyi, 'Állóképes Arckép Azonosítás Magyarországon [Still Image Face Recognition in Hungary]' (2020) 68(3) Belügyi Szemle 22, <https://doi.org/10.38146/BSZ.SPEC.2020.3.2>
- G Gültekin-Várkonyi, 'Navigating Data Governance Risks: Facial Recognition in Law Enforcement under EU Legislation' (2024) 13(3) Internet Policy Review <https://doi.org/10.14763/2024.3.1798>
- Graham Greenleaf, 'India's National ID System: Danger Grows in a Privacy Vacuum' (2010) Computer Law & Security Review 26(5), 479–491.
- Gültekin-Várkonyi G, 'Consent Mechanism in the Life with Social Robots' (2019) 31(1) European Review of Public Law.
- Hacker P, 'AI Regulation in Europe: From the AI Act to Future Regulatory Challenges' (2023) <https://doi.org/10.48550/arXiv.2310.04072> accessed 31 May 2025.
- HUMABIO Project, Human Monitoring and Authentication Using Biodynamic Indicators and Behavioral Analysis (EU Sixth Framework Programme, 2006–2008) http://cordis.europa.eu/fetch?CALLER=IST_UNIFIEDS-RCH&ACTION=D&DOC=6&CAT=PROJ&QUERY=011e5a6ef5cd:570d:08b193fe&RCN=78373 accessed 31 May 2025.
- I Fábíán and GG Gulyás, 'A Comparative Study on the Privacy Risks of Face Recognition Libraries' (2021) 25(2) Acta Cybernetica 233 <https://cyber.bibl.u-szeged.hu/index.php/actcybern/article/view/4198> accessed 1 June 2025.
- J R Matey et al, 'Iris on the Move: Acquisition of Images for Iris Recognition in Less Constrained Environments' (2006) Proceedings of the IEEE 1936–1947 <http://ieeexplore.ieee.org/Xplore/login.jsp?url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F5%2F4052463%2F04052478.pdf&authDecision=-203> ('Matey et al., Iris on the Move, 2006').
- Koops B-J, 'The Concept of Function Creep' (2021) 13(1) Law, Innovation and Technology 29 <https://doi.org/10.1080/17579961.2021.1898299> accessed 31 May 2025.
- L Basel-Vanagaite and others, 'Recognition of the Cornelia de Lange Syndrome Phenotype with Facial Dysmorphology Novel Analysis' (2016) 89(5) Clinical Genetics 557.

- L Urquhart and D Miranda, 'Policing Faces: The Present and Future of Intelligent Facial Surveillance' (2022) 31(2) Information & Communications Technology Law 194 <https://doi.org/10.1080/13600834.2021.1994220>
- Luke Scanlon, 'What Meaningful Human Oversight of AI Should Look Like' (2022) Pinsent Masons Out-Law <https://www.pinsentmasons.com/out-law/analysis/what-meaningful-human-oversight-of-ai-should-look-like>
- M Bromba, 'Reconstruction of Biometric Raw Data' (2006).
- N Helberger and N Diakopoulos, 'ChatGPT and the AI Act' (2023) 12(1) Internet Policy Review <https://doi.org/10.14763/2023.1.1682>
- Nathalie A Smuha and others, 'How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act' (2021) Social Science Research Network <https://doi.org/10.2139/ssrn.3899991>
- P Lewinski, J Trzaskowski and J Luzak, 'Face and Emotion Recognition on Commercial Property under EU Data Protection Law' (2016) 33(9) Psychology & Marketing 729.
- R Delikat, The Regulatory Gap Between the Law and the Use of Real-Time Facial Recognition Technology by Police in the European Union (Master's thesis, Tilburg University 2021) 61 <https://arno.uvt.nl/show.cgi?fid=155401> accessed 1 June 2025.
- R W Picard, 'Affective Computing: Challenges' (2003) 59(1) International Journal of Human-Computer Studies 55.
- Rainer Mühlhoff and Hannah Ruschemeier, 'Updating Purpose Limitation for AI: A Normative Approach from Law and Philosophy' (22 January 2024) SSRN <https://ssrn.com/abstract=4711621> or <http://dx.doi.org/10.2139/ssrn.4711621>
- Rezende IN, 'Facial Recognition in Police Hands: Assessing the "Clearview Case" from a European Perspective' (2020) 11(3) New Journal of European Criminal Law 375 <https://doi.org/10.1177/2032284420948161> accessed 31 May 2025.
- RP Kosilek and others, 'Automatic Face Classification of Cushing's Syndrome in Women – A Novel Screening Approach' (2013) 121(9) Experimental and Clinical Endocrinology & Diabetes 561.

- RSS Kramer, MO Mireku, TR Flack and others, 'Face Morphing Attacks: Investigating Detection with Humans and Computers' (2019) 4 Cognitive Research 28 <https://doi.org/10.1186/s41235-019-0181-4>
- S Khairnar, S Gite, K Kotecha and SD Thepade, 'Face Liveness Detection Using Artificial Intelligence Techniques: A Systematic Literature Review and Future Directions' (2023) 7(1) Big Data and Cognitive Computing 37 <https://doi.org/10.3390/bdcc7010037>
- Sandra Wachter, 'Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond' (2024) 26(3) Yale Journal of Law & Technology <https://ssrn.com/abstract=4924553> or <http://dx.doi.org/10.2139/ssrn.4924553>
- T Züger and H Asghari, 'AI for the Public: How Public Interest Theory Shifts the Discourse on AI' (2023) 38 AI & Society 815 <https://doi.org/10.1007/s00146-022-01480-5>
- Tim Miller, 'Explanation in Artificial Intelligence: Insights from the Social Sciences' (2019) 267 Artificial Intelligence 1 <https://www.sciencedirect.com/science/article/pii/S0004370218305988>
- U Park, Y Tong and AK Jain, 'Face Recognition with Temporal Invariance: A 3D Aging Model' (2010) IEEE Transactions on Pattern Analysis and Machine Intelligence 32(5), 947 <https://ieeexplore.ieee.org/document/5413023> accessed 1 June 2025.
- VL Raposo, '(Do Not) Remember My Face: Uses of Facial Recognition Technology in Light of the General Data Protection Regulation' (2023) 32(1) Information & Communications Technology Law 45 <https://doi.org/10.1080/13600834.2022.2054076> accessed 1 June 2025.
- Yichao Ma, Zengxi Huang, Xiaoming Wang and Kai Huang, 'An Overview of Multimodal Biometrics Using the Face and Ear' (2020) Mathematical Problems in Engineering <https://doi.org/10.1155/2020/6802905>
- Yuncong Yang and others, 'From Machine Learning to Machine Unlearning: Complying with GDPR's Right to be Forgotten while Maintaining Business Value of Predictive Models' (2024) arXiv preprint arXiv:2411.17126 <https://arxiv.org/pdf/2411.17126>

• International Legal Documents:

- Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies (WP 193, 27 April 2012).

- Article 29 Data Protection Working Party, Working Document on Biometrics, WP 80, 1 August 2003, 11 ('WP 29 Working Document on Biometrics 2003 (WP80)'); Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies, WP 193, 27 April 2012.

- Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

- Commission Decision of 28 June 2006 laying down the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States.

- Consultative Committee of the Convention 108, Guidelines on Facial Recognition (Guideline No T-PD(2020)03rev4, Council of Europe 2021) <https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html> accessed 31 May 2025.

- Convention for the Protection of Human Rights and Fundamental Freedoms, Protocol No 12 (opened for signature 4 November 2000, entered into force 1 April 2005).

- Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR).

- Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Modernised Convention 108, 2018).

- EDPS (European Data Protection Supervisor), Opinion on the Proposal for a Council Decision on the establishment, operation and use of the second-generation Schengen Information System (SIS II) (2005) 19.

- European Commission, Convergence: Creating the Future Commission. President Jacques Santer Announces 200,000 ECU European IT Prize Winners (25 November 1997) <http://cordis.europa.eu/esprit/src/eitcp4en.htm> accessed 31 May 2025.

- European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), COM/2021/206 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>
- European Commission, Shaping Europe's Digital Future (February 2020) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0067>
- European Commission, White Paper on Artificial Intelligence – A European Approach to Excellence and Trust, COM(2020) 65 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0065>
- European Data Protection Board and European Data Protection Supervisor, Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) (18 June 2021) https://www.edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf
- European Data Protection Board, 'Facial Recognition: Italian SA Fines Clearview AI EUR 20 Million' (2022) https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en accessed 31 May 2025.
- European Data Protection Board, Guidelines 05/2020 on Consent under Regulation 2016/679 (May 2020) 7–32 https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf accessed 31 May 2025.
- European Data Protection Board, Guidelines 3/2019 on Processing of Personal Data Through Video Devices (January 2020) 5–23 https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices.pdf accessed 31 May 2025.
- European Data Protection Board, Swedish DPA: Police Unlawfully Used Facial Recognition App (Press release, 2021) https://www.edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en accessed 31 May 2025.

- European Parliament, Amendments Adopted by the European Parliament on 14 June 2023 on the Proposal for a Regulation of the European Parliament and of the Council on Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (2023) https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html

- European Union Agency for Fundamental Rights, *Handbook on European Data Protection Law: 2018 Edition* (FRA, 2018) https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf accessed 31 May 2025.

- International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR).

- Regulation (EC) No 2252/2004 of 13 December 2004 on Standards for Security Features and Biometrics in Passports and Travel Documents Issued by Member States [2004] OJ L385/1.

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) <https://eur-lex.europa.eu/eli/reg/2016/679/oj> accessed 31 May 2025.

- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689 accessed 31 May 2025.

• **Laws:**

- Act CCXXII of 2015 (Hungary) <https://njt.hu/jogszabaly/en/2015-222-00-00>

• Reports:

- van der Wolk and Morrison & Foerster, 'The (Im)Possibilities of Scientific Research Under the GDPR' (Cybersecurity Law Report, 2020) 3–4 <https://assets.contentstack.io/v3/assets/blt5775cc69c999c255/bltbb2bb3d-f1bea55fe/200722-scientific-research-gdpr.pdf> accessed 31 May 2025.
- Amba Kak, Regulating Biometrics: Global Approaches and Open Questions (AI Now Institute 2020) <https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions>
- American Society for Testing and Materials, Standard Guide for Capturing Facial Images for Use with Facial Recognition Systems (ASTM International, 2023) Vol 14.02, No E3115-17 <https://doi.org/10.1520/E3115-17> accessed 1 June 2025.
- Amnesty International, 'EU: Artificial Intelligence Rulebook Fails to Stop Proliferation of Abusive Technologies' (Amnesty International, 14 March 2024) <https://www.amnesty.org/en/latest/news/2024/03/eu-artificial-intelligence-rulebook-fails-to-stop-proliferation-of-abusive-technologies/>
- Andy Ashbourn, Social Implications of Wide Scale Implementation of Biometrics (2005) 6.
- Banda J, 'Inherently Identifiable: Is It Possible to Anonymize Health and Genetic Data?' (IAPP, 13 November 2019) <https://iapp.org/news/a/inherently-identifiable-is-it-possible-to-anonymize-health-and-genetic-data> accessed 31 May 2025.
- E Garvie, A Bedoya and J Frankle, The Perpetual Line-Up: Unregulated Police Face Recognition in America [Report] (Center on Privacy & Technology at Georgetown Law 2016) <https://www.perpetuallineup.org/risk-framework>
- E Jakubowska, Remote Biometric Identification: A Technical & Legal Guide [Guidance] (European Digital Rights 2023) <https://edri.org/our-work/remote-biometric-identification-a-technical-legal-guide/>
- E Moss and others, Assembling Accountability: Algorithmic Impact Assessment for the Public Interest (Data & Society 2021) <https://datasociety.net/library/assembling-accountability-algorithmic-impact-assessment-for-the-public-interest/>

- Europol, ChatGPT: The Impact of Large Language Models on Law Enforcement (Tech Watch Flash) (Europol Innovation Lab, 2023) <https://www.europol.europa.eu/publications-events/publications/chatgpt-impact-of-large-language-models-law-enforcement> accessed 31 May 2025.
- Gary Roethenbaugh, cited in A Cavoukian, Privacy and Biometrics (Information and Privacy Commissioner, Ontario 1999) 11 <http://www.ipc.on.ca/images/Resources/pri-biom.pdf> accessed 31 May 2025.
- Joseph Pato and Lynette Millett (eds), Biometric Recognition: Challenges and Opportunities (National Research Council, September 2010) 3 ('NRC, Biometric Recognition, 2010').
- Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (Conference on Fairness, Accountability, and Transparency, 2018) <https://www.media.mit.edu/publications/gender-shades-intersectional-accuracy-disparities-in-commercial-gender-classification/> accessed 1 June 2025.
- M Gasson, M Meints and K Warwick (eds), D.3.2: A Study on PKI and Biometrics (FIDIS, Frankfurt, July 2005) 82–86.
- Michael Gasson, Martin Meints and Kevin Warwick (eds), D3.2 A Study on PKI and Biometrics, FIDIS (2005) <http://www.fidis.net/resources/fidis-deliverables>
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Kamerstuk 25 764, nr. 27b1 (2005) 83 <https://zoek.officielebekendmakingen.nl/kst-25764-27-b1.pdf> accessed 1 June 2025.
- National Institute of Standards and Technology (NIST), 'NIST Evaluates Face Recognition Software's Accuracy for Flight Boarding' (17 July 2021) <https://www.nist.gov/news-events/news/2021/07/nist-evaluates-face-recognition-software-accuracy-flight-boarding> accessed 1 June 2025.
- National Institute of Standards and Technology (NIST), 'NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software' (19 December 2019) <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software>
- National Science and Technology Council (NSTC), Palm Print Recognition (2006). <http://www.biometrics.gov/documents/palmprintrec.pdf>.

- Organization for Economic Co-operation and Development, Biometric-based Technologies (OECD, DSTI/ICCP/REG(2003)2/FINAL, 30 June 2004, cancelling and replacing the same document of 28 April 2004) 11 ('OECD, Biometric-based technologies, 2004').
- Reva Schwartz and others, Towards a Standard for Identifying and Managing Bias in Artificial Intelligence (NIST Special Publication 1270, 2022).
- Tambiama Madiaga and Hendrik Mildebrath, Regulating Facial Recognition in the EU (European Parliamentary Research Service 2021) [https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA\(2021\)698021_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf)
- Theodore Christakis, Mathias Becuywe and AI-Regulation Team, Facial Recognition in the Draft European AI Regulation: Final Report on the High-Level Workshop Held on April 26, 2021 (2021) <https://ai-regulation.com/wp-content/uploads/2021/05/Final-Report-26-04.pdf>
- Theodore Christakis, Mathias Becuywe and AI-Regulation Team, Facial Recognition in the Draft European AI Regulation: Final Report on the High-Level Workshop Held on April 26, 2021 (AI-Regulation.com 2021) <https://ai-regulation.com/facial-recognition-in-the-draft-european-ai-regulation-final-report-on-the-high-level-workshop-held-on-april-26-2021/>
- TIPIK Legal, Report on the Implementation of Specific Provisions of Regulation (EU) 2016/679 [Final report] (European Commission Directorate General for Justice and Consumers Unit C.3 Data Protection 2021) <https://www.dataguidance.com/sites/default/files/1609930170392.pdf>
- UK National Cyber Security Centre, Biometrics: Measuring Performance (2019) <https://www.ncsc.gov.uk/collection/biometrics/measuring-performance#:~:text=A%20false%20match%20occurs%20when,a%20characteristic%20from%20another%20individual> accessed 31 May 2025.
- UK Passport Service, Biometrics Enrolment Trial (May 2005) 299.
- World Bank, Practitioner's Guide: Biometric Data, Identification for Development (ID4D) <https://id4d.worldbank.org/guide/biometric-data>

• Conferences:

- A Kartali, M Roglic, M Barjaktarovic, M Duric-Jovicic and M M Jankovic, 'Real-time Algorithms for Facial Emotion Recognition: A Comparison of Different Approaches' (2018) 14th Symposium on Neural Networks and Applications (NEUREL) 1.

- AS Bergman and others, 'Representation in AI Evaluations' in Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency (2023) 519 <https://dl.acm.org/doi/fullHtml/10.1145/3593013.3594019> accessed 1 June 2025.

- Daniel Florez Mendez and others, 'Facial Recognition System for Security Access Control' (2021) 11842 Proceedings of SPIE: Applications of Digital Image Processing XLIV 1184217.

- E Bondi and others, 'Envisioning Communities: A Participatory Approach Towards AI for Social Good' (2021) Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society 425 <https://doi.org/10.1145/3461702.3462612>

- G Udovičić, J Đerek, M Russo and M Sikora, 'Wearable Emotion Recognition System Based on GSR and PPG Signals' in Proceedings of the 2nd International Workshop on Multimedia for Personal Health and Health Care (MMHealth '17) (Association for Computing Machinery, New York, NY, USA, 2017) 53.

- Kanubhai K Patel, Jignesh J Patoliya and Miral M Desai, 'IoT Based Smart Health Monitoring System with Patient Identification Using Face Recognition' in Proceedings of the International Conference on Innovative Computing & Communication (ICICC, 2021).

- M Sloane and others, 'Participation Is Not a Design Fix for Machine Learning' (2022) Proceedings of the 2nd ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization 1 <https://doi.org/10.1145/3551624.3555285>

P Tuyls, E Verbitskiy, T Ignatenko, D Schobben and T Akkermans, Privacy Protected Biometric Templates: Acoustic Ear Identification (paper submitted at SPIE 2004) <http://www.sps.ele.tue.nl/members/T.Ignatenko/papers/SPIE2004.pdf> accessed 31 May 2025.

- Speech Technology Center, Voice Biometrics: Exciting Capabilities of a New Biometric Modality (presentation at Rise and Hide Conference, Brussels, 9–10 December 2010) slides 2, 4 and 14 http://www.riseproject.eu/_file-

[upload/RISE%20Conference/Presentations/Alexey%20Khitrov.pdf](https://www.rise.ac.uk/Conference/Presentations/Alexey%20Khitrov.pdf) accessed 31 May 2025.

- Wang Y-F, Chang EY and Cheng KP, 'A Video Analysis Framework for Soft Biometry Security Surveillance' in Proceedings of the Third ACM International Workshop on Video Surveillance & Sensor Networks (2005) 71 <https://doi.org/10.1145/1099396.1099412> accessed 31 May 2025.

- Y Zhou and A Kumar, 'Contactless Palm Vein Identification Using Multiple Representations' (presentation and paper, IEEE Fourth International Conference on Biometrics: Theory, Applications and Systems (BTAS 2010), Washington DC, 27–29 September 2010) 6.

• Case Law:

- Bridges v Chief Constable of South Wales Police [2019] EWHC 2341 (Admin) <https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf> accessed 31 May 2025.

- Dimitrov-Kazakov v Bulgaria (Application No 11379/03, ECtHR, 2018) <https://hudoc.echr.coe.int/eng?i=001-103258> accessed 31 May 2025.

- S and Marper v United Kingdom App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008) <https://hudoc.echr.coe.int/fre?i=001-90051>

• Websites:

- Arno Cuypers, 'The Right to Explanation in the AI Act: A Right to Interpretable Models?' (2024) CiTiP Blog, KU Leuven <https://www.law.kuleuven.be/citip/blog/the-right-to-explanation-in-the-ai-act-a-right-to-interpretable-models/>

- ARTICLE 19, 'EU: AI Act Passed in Parliament Fails to Ban Harmful Biometric Technologies' (ARTICLE 19, 13 March 2024) <https://www.article19.org/resources/eu-ai-act-passed-in-parliament-fails-to-ban-harmful-biometric-technologies/>

- Barak Bassman and others, 'Facing Up to Tough Issues: Health Care Compliance Concerns with Facial Recognition Technology' (JDSupra, 12 May 2021) <https://www.jdsupra.com/legalnews/facing-up-to-tough-issues-health-care-9118586/> accessed 31 May 2025.

- C Helleputte, S Belotti and F Cieri, 'The Italian DPA Has Its Eyes on Biometric IDs – Another Fight on Tech or a Win for Privacy?' (Privacy World, 9 April 2024) <https://www.privacyworld.blog/2024/04/the-italian-dpa-has-its-eyes-on-biometric-ids-another-fight-on-tech-or-a-win-for-privacy/>

- E Moss and J Metcalf, 'The Ethical Dilemma at the Heart of Big Tech Companies' (Harvard Business Review, 14 November 2019) <https://hbr.org/2019/11/the-ethical-dilemma-at-the-heart-of-big-tech-companies>
- E Sherwin and E Baryshewa, 'Russian Court Rejects Facial Recognition - Technology Ban' (DW News, 11 June 2019) <https://www.dw.com/en/russian-court-rejects-call-to-ban-facial-recognition-technology/a-51135814>
- Federal Bureau of Investigation, Statement on Brandon Mayfield Case (24 May 2004) <https://archives.fbi.gov/archives/news/pressrel/press-releases/statement-on-brandon-mayfield-case>
- Future of Life Institute, 'The Act Texts' (Future of Life Institute, 2024) <https://artificialintelligenceact.eu/theact/>
- Hill K, 'Wrongfully Accused by an Algorithm' New York Times (24 June 2020) <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html> accessed 31 May 2025.
- International Organization for Standardization (ISO), ISO/IEC 2382-37:2022 – Information Technology – Vocabulary – Part 37: Biometrics (2022–23) <https://www.iso.org/standard/73514.html> accessed 31 May 2025.
- Johannes Walter, 'Human Oversight Done Right: The AI Act Should Use Humans to Monitor AI Only When Effective' (2023) ZEW Policy Briefs 02/2023, ZEW – Leibniz Centre for European Economic Research https://www.zew.de/en/publications/human-oversight-done-right-the-ai-act-should-use-humans-to-monitor-ai-only-when-effective-1?utm_source=chatgpt.com#publication532409
- Laura Caroli, 'Will the EU AI Act Work? Lessons Learned from Past Legislative Initiatives, Future Challenges' (International Association of Privacy Professionals, 17 April 2024) <https://iapp.org/news/a/will-the-eu-ai-act-work-lessons-learned-from-past-legislative-initiatives-future-challenges>
- M Borak, 'Police in Germany Using Live Facial Recognition' (8 May 2024) Biometric Update <https://www.biometricupdate.com/202405/police-in-germany-using-live-facial-recognition> accessed 31 May 2025.
- NOYB – European Center for Digital Rights, 'Clearview AI Data Use Deemed Illegal in Austria, However No Fine Issued' (2023) <https://noyb.eu/en/clearview-ai-data-use-deemed-illegal-austria-however-no-fine-issued> accessed 31 May 2025.
- Office of Biometric Identity Management, Biometrics (US Department of

Homeland Security) <https://www.dhs.gov/biometrics> accessed 31 May 2025.

- Oxford Reference, 'Socio-technical System' <https://www.oxfordreference.com/display/10.1093/oi/authority.20110803100515814> accessed 1 June 2025.

- Phillip Hacker, 'Comments on the Final Trilogue Version of the AI Act' (European New School, 23 January 2024) <https://www.europeannewschool.eu/images/chairs/hacker/Comments%20on%20the%20AI%20Act.pdf>

- Simona Demkova, 'The AI Act's Right to Explanation: A Plea for an Integrated Remedy' (2024) MediaLaws <https://www.medialaws.eu/the-ai-acts-right-to-explanation-a-plea-for-an-integrated-remedy/>

- Vocabulary.com, 'Vulnerability' <https://www.vocabulary.com/dictionary/vulnerability> accessed 31 May 2025.