كيفية استخدام تقنية بصمة الوجه الرقمية كنشاط تحقيقي عملي في الإجراءات الجنائية المعاصرة: تحليل نقدي مقارن لمشروع جرائم المعلوماتية العراقية

فهيل عبد الباسط عبد الكريم

قسم الادارة القانونية، كلية التقنية الادارية، جامعة دهوك التقنية، كوردستان، العراق

المستخلص

بصمة الوجه الرقمية في علم الاجرام الخوارزمي تعد دليلا رقميا مفرزا من الثورة الصناعية الرابعة واستخدام خوارزميات الذكاء الاصطناعي للتعرف الى الوجه رقميا، بالاستعانة بكاميرات الرصد والمراقبة والتقنيات الحديثة الاخرى. فمن بين تفاصيل التي يتضمنها هذه البصمة، ملامح الوجه (الاذنين والفم والشفتين والعينين والذقن والوجنتين)، وهذه الملامح بدورها منفصلا تعد هي الاخر من الادلة العلمية التقليدية في الاثبات الجنائي. من المعلوم، بانه حاليا يتم استخدام هذه التقنية في مختلف المجالات، للتحقق من شخصية الفرد (الهوية الشخصية) في مراكز التفتيش في المطارات ونقاط الحدود وماكينات الصرف الالي. وتمثل اشكالية الدراسة في استخدام التقنية المذكورة كنتيجة لنشاط تحقيقي عملي في الاجراءات الجنائية المعاصرة، وبالتحديد في الاثبات الجنائي. ومن ثم ابراز قيمتها الثبوتية في الاجراءات الجنائية المعاصرة، بالاعتماد على المنهج الوصفي والمنهج التحليلي. وتهدف الدراسة الى معرفة تقنية بصمة الوجه الرقمية من منظورها القانوني، ومن ثم بيان اهمية استخدام نتائج هذه التقنية كنشاط تحقيقي عملي في هذه الاجراءات الجنائية المعاصرة، مستعرضا حجية الآراء المؤيدة والآراء المعارضة لاستخدام نتائج هذا النشاط. وفي الخاتمة، توصلت الدراسة الا ان لبصمة الوجه الرقمية دور بارز في مجال الاثبات الجنائي، بالإضافة الى دورها الوقائي (التنبؤي) في مكافحة الجريمة في مجال الضبط الاداري. كما وتوصي الدراسة على انه يجب ان يكون غاية ووسيلة استخدام نتائج بصمة الوجه الرقمية مشروعة وتم أخذها في مكان عام، مراعيا حق الفرد في الخصوصية الشخصية وحرمة الحياة الخاصة، كما وتوصلت الدراسة الى اهمية التثقيف الرقمي لرجال الضبط القضائي والتحقيق (رجال انفاذ القانون) وتلقينهم تقنيا عن طريق عقد دورات تقنية-قانونية متخصصة من قبل المختصين في مجال العلم القانوني البيني (اي ما بين علم القانون وعلم التكنولوجيا الرقمية).

الكلمات المفتاحية: بصمة الوجه الرقمية، مكافحة الجريمة، الاثبات الجنائي، الدليل الرقمي، النشاط التحقيقي العملي، قانون الجرائم الالكترونية

1. المقدمة

بعد ان تم استحداث وسائل التكنولوجيا الرقمية باستخدامها على سرعة انجاز المعاملات اليومية، من خلال اثبات الهوية الشخصية للأفراد وبدقة عالية. فتم استغلال هذه التقنية بمفهومها الجديد نسبيا في عام 1960 كأول نظام ألي للتعرف على الوجه، من خلال تحديد الابعاد الاساسية في الوجه كالعينين ووضعية الفم والانف للأفراد وقتذاك. ومن ثم تم الاستعانة بهذه التقنية في مجالات متعددة للتحقق من الهوية الشخصية في المطارات ونقاط التفتيش الحدودية، بالإضافة الى ماكينات الصرف الالي للتعرف الى العملاء عن طريق هذه التقنية .

تقنية بصمة الوجه الرقمية هي تقنية احتمالية مصممة للتعرف آليًا على الأفراد بالاعتماد على وجوههم بهدف التحقق من الهوية أو التعرف عليهم أو تحديدهم. يسمح بمقارنة صور الوجه الرقمية، التي تُجمع عبر كاميرات الفيديو الحية (closed-circuit television (CCTV))أو الصور، لتحديد ما إذا كانت الصور المقارنة تعود لنفس الفرد. يسمى قياس اللقطات التي تم الحصول عليها من CCTV بالصور الموجودة في قواعد البيانات بتقنية التعرف على الوجه المباشر (live facial recognition

مجلة جامعة جيهان- اربيل للعلوم الانسانية والاجتماعية
المجلد 9، العدد 2 (2025).
أُستلم البحث في 3 أيار 2025؛ قُبل في 6 أيلول 2025
ورقة بحث منتظمة: نُشرت في 10 تشرين الأول 2025
البريد الإلكتروني للمؤلف:fahil.abdulbasit@dpu.edu.krd

10.24086/cuejhss.v9n2y2025.pp89-95

technology (LFR).عندما تُستخدم مقاطع الفيديو مع التأثير الاسترجاعي من جانب البيانات التي تم جمعها سابقًا في قاعدة البيانات، يطلق عليها اسم التعرف على الوجه بأثر رجعي (retrospective facial recognition (RFR)). علاوة على ذلك، تُعرف تطبيقات الأجهزة المحمولة التي تسمح بتصوير الأفراد والتحقق من هويتهم باسم المشغل الذي بدأ التعرف على الوجه (operator initiated facial recognition (OIFR)).

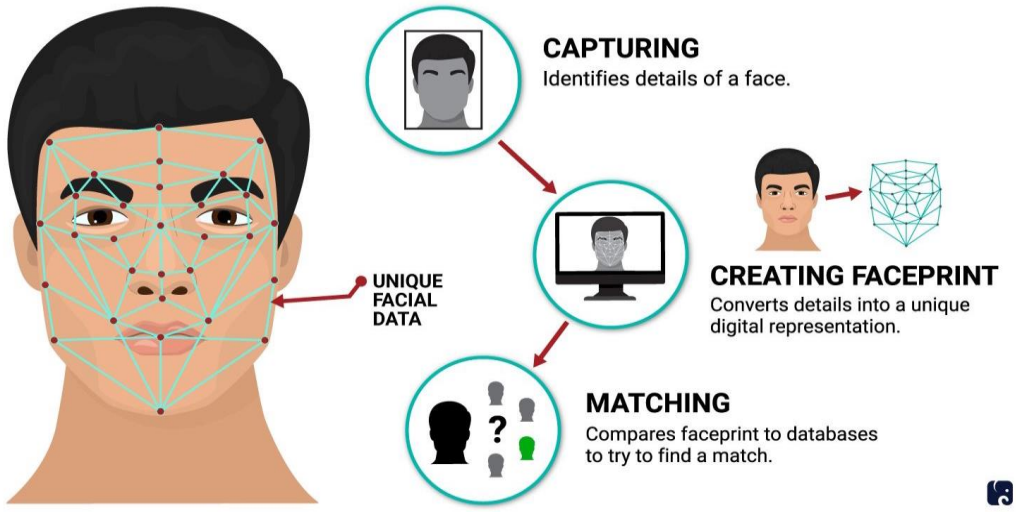
وبالرغم من اختلاف طريقة التعرف الالكتروني الى الوجه وذلك بحسب منهجية البرنامج المستخدم، ولكن بشكل عام يجري العمل وفق خطوات متسلسلة ومحددة للتعرف على ما يقارب 80 نقطة عقدية، هذه النقاط التي تشكل الارتفاعات والانخفاضات ملامح وجه الفرد، متمثلا بالمسافة بين العينين ووضعية ومساحة الانف وعمق التجويف العيني وتوضع الخدود وخطوط الذقن والفك السفلي. ومنهجية جميع البرامج يستهل بالخطوات الثلاثة الاساسية التالية: التقاط الصورة ومن ثم خطوة التحليل والمعالجة وفي النهاية خطوة المقارنة، اي معالجة الصورة الملتقطة في قاعدة البيانات الضخمة. الاهمية النظرية للدراسة تكمن في ضرورة اعتماد تقنية بصمة الوجه الرقمية في التعرف على وجوه المجرمين والمطلوبين في مجال مكافحة الجريمة (T. L. Johnson et al., 2022)، والاهمية العملية (في مجال التحقيق) تكمن في القيمة الثبوتية العالية لهذه التقنية في مجال الاثبات الجنائي، مع أخذ التحديات التي بات تشكلها هذه التقنية على الخصوصية الشخصية وحرمة الحياة الخاصة للفرد بعين الاعتبار. وبالتالي تقنية بصمة الوجه الرقمية، وكما هو مع مزايا كل تقنية حديثة، هناك قلق وتحديات واسعة النطاق تواجه المجتمع والقانون. من الناحية القانونية، تنشأ هذه المخاوف فيما يتعلق بحق الفرد في حياته الخاصة وحماية خصوصيته، وكذلك التمييز، والجريمة، وسيادة القانون، والمبادئ الدستورية الجوهرية. وتترافق هذه المخاوف أيضًا مع مسألة المسؤولية، لا سيما في غياب أطر قانونية شاملة لمراقبة وتنظيم استعمال هذه التقنيات المستحدثة وآثارها. فموضوع البحث يتناول الجدل المحتدم حول ضرورة سنّ قانون للتعامل مع تبعاتها الظاهرة

2. تعريف بصمة الوجه الرقمية

بالرغم من ان المشرع الجنائي العراقي لم يتعرض لتعريف بصمة الوجه الرقمية في مفهوم تشريعي محدد في مشروع قانون جرائم المعلوماتية، كل ذلك بحسب رأي الباحث، من اجل ان لا يتم تقيد هذه التقنية الرقمية بمنهجية محددة، هذا من جانب ومن جانب اخر لكي يتم افساح المجال للفقه الجنائي باستيعاب التحديثات التقنية المستقبلية لبصمة الوجه الرقمية المستخدمة ضمن مفهومها التعريفي الواسع لنشاط التحقيقي العملي .

وبشكل عام، تعرف بصمة الوجه الرقمية (Abudarham, Grosbard, & Yovel, 2021) بأنها: عبارة عن برنامج قادر على تحديد الوجوه الموجودة في الصورة، وجعلها مميزة عن باقي الاجزاء في الصورة الواحدة، ومن ثم يقوم بمقارنة هذا الوجه مع قاعدة البيانات المملوءة بصور لوجوه العديد من الاشخاص، حيث يوجد في الوجه العديد من المناطق المميزة عن غيرها، فبعضها مرتفع عن سطح الوجه، وبعضها الاخر منخفض، هذه الارتفاعات والانخفاضات تشكل ملامح الوجه. أي يتم التقاط الصورة بواسطة الكاميرا (التصوير الفوتوغرافي أو التصوير السينمائي Photography or Cinematography) هذه الارتفاعات والانخفاضات بنقاط عقدية (تقريبا 80 نقطة عقدية في الوجه) لتكون بعد ذلك بصمة الوجه، ومن ثم تحويل تفاصيل الوجه هذه خوارزميا إلى تمثيل رقمي فريد (بيانات الوجه الفريدةUnique Facial Data)، وبعد ذلك يتم مرحلة المطابقة، أي مقارنة بيانات الوجه الفريدة هذه (التمثيل الرقمي الفريد) في قاعدة البيانات للعثور على التطابق. لذا تتكون أنظمة بصمة الوجه الرقمية عادةً من 3 مكونات: الكاميرا والخوارزمية (البرنامج الخوارزمي) وقاعدة البيانات، وقد يكون نظام بصمة الوجه الرقمية أيضًا برنامجًا مكتملا مترابطا واحدا. وتعتمد تقنية بصمة الوجه الرقمية على التعلم الآلي (Machine Learning) التعلم الآلي (Tripathi, 2017)، كفرع من الذكاء الصناعي يسمح للحواسيب بالتعلم من البيانات وتحسين أدائها مع مرور الوقت دون الحاجة إلى برمجتها بشكل مباشر لكل مهمة، وذلك من خلال الخوارزميات المصممة لجمع واكتشاف المعلومات والسمات البيومترية من خلال الاستخراج التلقائي (الاسترجاعي) والتوزيع الهندسي المكاني والعددي للملامح الوجه (Sajta, n.d.). التعلم الآلي والتعلم الآلي العميق هي تقنيات تُستخدم لتحليل المتغيرات المعقدة والبيانات الضخمة. من الناحية التقنية، يمكن الإشارة إلى خوارزمية التعرف على الوجه على أنها عملية أو مجموعة من القواعد التي يجب اتباعها لحساب أو تحليل ملامح الوجه باستخدام الحاسوب (Berle, 2020) (انظر الشكل 1 (Factsheet: Facial Recognition Technology (FRT).

الشكل:1 تقنية التعرف على الوجه



2.1 مميزات بصمة الوجه الرقمية كونها بصمة غير وراثية

من حيث الطبيعة: نظرا لكون البصمة الوراثية بالاساس مبنية على اساس وراثي، يستمده الفرد من أبويه، في حين بصمة الوجه الرقمية مبنية بالأساس على أساس تقني ولا تتأثر غالبا بالعوامل الوراثية(Lois & Groves, 2011)

من حيث الوظيفة: بالرغم من أن البصمة الوراثية وبصمة الوجه الرقمية تتلاقيان في مجال تحقيق شخصية الفرد، الا انهما تختلفان في الوظائف الاخرى، فمثلا إثبات النسب، الجنسية، التعرف على المفقودين وضحايا الحروب والكوارث، الجرائم الجنسية والاغتصاب، البحوث العلمية، تشخيص ومعالجة الامراض الوراثية ومعرفة أصول النباتات والحيوانات، ففي جميع الحالات السابقة لايتم الاستعانة الا بالبصمة الوراثية، بينما بصمة الوجه الرقمية (موضوع البحث) كونها ذي طبيعة غير وراثية لا يتمتع بالميزة الوظيفية المذكورة؛

من حيث القيمة الثبوتية: القيمة الثبوتية لبصمة الوجه الرقمية تكمن في معرفتها للوجه وبالتالي إثبات الهوية الشخصية للفرد، معتمدا على الشكل الخارجي للوجه بملامحه المميزة لها، بينما البصمة الوراثية تعتمد على تحليل الحمض النووي (DNA) للفرد جزئيا أو كليا (Michalski et al., 2024).

3. مشروعية (حجية) بصمة الوجه الرقمية في الاثبات الجنائي

3.1 الاتجاه المؤيد لاستخدام بصمة الوجه الرقمية كنشاط تحقيقي عملي

ويدعم هذا الاتجاه استخدام تقنية التعرف الرقمي على الوجه كنشاط تحقيقي عملي للتعرف على الجناة، استنادًا إلى مبدأ شرعية الأدلة الجنائية، وأن هذا الاستخدام يمكن أن يؤدي إلى قمع الجريمة ومنعها .(Dessimoz & Champod, 2015) لا يحظر القانون التصوير في الأماكن العامة طالما أنه لا ينتهك حق الفرد في الخصوصية أو الحياة الخاصة. ويدعم نظام العدالة الجنائية الروسي هذا الاتجاه طالما أن هذا النشاط يحترم المبادئ الدستورية الأربعة الواردة في القانون الاتحادي الروسي الصادر في 12 أغسطس 1995 (مجلس الدوما، 1995) رقم 144 FZ-بصيغته المعدلة في 29 ديسمبر 2022 (“Federal'nyj Zakon ‘Ob Operativno-rozysknoj Dejatel'nosti’ Ot 12.08.1995 N 144-FZ (Poslednjaja Redakcija) \ Konsul'tantPljus,” n.d.).

المبدأ الأول: تمثل المشروعية في الامتثال غير المشروط والصارم لقواعد القانون الأساسي ودستور الاتحاد الروسي وتنفيذ توجيهاته من قبل القائمين بأنشطة التحقيق الفعلية. كما أنها تمثل في الامتثال لتطبيق القوانين المعيارية الأخرى التي تنظم آليات القيام بأنشطة التحقيق العملي.

المبدأ الثاني: وبالتالي فإن التقاط الصور الفوتوغرافية في الأماكن العامة دون موافقة الشخص لا يشكل انتهاكاً للحق في احترام الحياة الخاصة. ومع ذلك، ينبغي التمييز بين حالتين للتصوير الفوتوغرافي والمراقبة (التعرف الرقمي على الوجه) في الأماكن العامة. الحالة الأولى: حيث يكون المكان العام هو الهدف الرئيسي للتصوير أو المراقبة. الحالة الثانية: حيث يكون الشخص هو الهدف الرئيسي للتصوير أو المراقبة. في هذه الحالة، يكون الفعل غير قانوني. وذلك لأنه، على الرغم من أن وجود الشخص في المكان العام لا يمنع امتداد النظرة، إلا أنه بالنظر إلى الديمومة التي يضفيها هذا الفعل على النظر اللحظي، ينبغي مع ذلك الاعتراف بسلطة الطعن في كون الشخص هو الهدف الرئيسي للفعل.

المبدأ الثالث: مبدأ عدم التأمر (التواطؤ)، يعني الدعم التآمري (التواطئي) لحل التحديات التشغيلية لأنشطة التحقيق العملياتي. يضمن مبدأ عدم التأمر الحفاظ على سرية المعلومات المتعلقة بأسرار الدولة والأسرار العامة الأخرى، وغيرها من المعلومات التي يتعين فك شيفرتها، وبالتالي القضاء على إمكانية استخدامها ضد مصالح وكالات إنفاذ القانون، أي التأمر ضدها. وبعبارة أخرى، فإن مفهوم عدم التأمر هو الحفاظ على سرية الجوانب التنظيمية والتكتيكية لتنفيذ أنشطة التحقيق العملياتي - قواتها ووسائلها وأساليبها.

المبدأ الرابع:الجمع بين الطرق والوسائل العامة والخاصة، أي استخدام التقنيات والمنهجيات لحل المشكلة عند القيام بأنشطة التحقيق العملية علناً أو سراً. ويشكل مبدأ الجمع بين الطرق والوسائل العامة في جوهره وغرضه استمراراً وتطويراً لمبدأ عدم التأمر من خلال إتاحة الفرصة للتمييز بين المعلومات المتاحة للعموم والمعلومات السرية التي لا تخضع للنشر، أو المعلومات المحمية دستورياً. فمن ناحية أخرى، يتيح هذا المبدأ إمكانية التمييز بين مختلف أنواع الأنشطة التي تقوم بها مختلف وكالات إنفاذ القانون في مجال مكافحة الجريمة سراً أو علناً.

3.2 الاتجاه الرافض لاستخدام بصمة الوجه الرقمية كنشاط تحقيقي عملي

بالاستناد الى المبدأ الدستوري المتعلق بحق الفرد في الخصوصية الشخصية وحقه في الحياة الخاصة، هذا الاتجاه يتمسكه بعدم مشروعية بصمة الوجه الرقمية، ومن ثم عدم مشروعيته كدليل رقمي في النشاط التحقيقي العملي، يدعي بأن هذا النشاط بالأساس أتى من جراء الاعتداء على خصوصية الفرد المراقب (T. L. Crawford, 2019) (Johnson et al., 2024). إلا أن هذه المعارضة لم يأتي بشكل مطلق وإنما أجاز مناصرو هذا الاتجاه النشاط متى ما توفرت الضمانات الدستورية في إجراءات التحقيق العملي، وتمسكهم بهذا الشرط يأتي لغلق الطريق أمام السلطات الامنية إحتمالية استغلال هذا النشاط تحت طائلة تحقيق العدالة، والتي لا ينبغي للعدالة أن تكون جديرة بهذا الاسم .(Allyn, 2020) (Lai & Rau, 2021)

في هذا السياق، تجدر الإشارة إلى قرار البرلمان الأوروبي بشأن الذكاء الاصطناعي، وتحديدًا استخدامه في القانون الجنائي ومن قِبل الشرطة والسلطات القضائية في المسائل الجنائية، مع التركيز بشكل خاص على تقنية بصمة الوجه الرقمية .(FRT) إذ ينص القرار على ما يلي:

"نظرًا إلى أنَّ لأنواع استخدامات تقنية التعرف على الوجوه (بصمة الوجه الرقمية) آثارًا متباينة على حماية الحقوق الأساسية، ينبغي أن يقتصر استخدامها من قِبل جهات إنفاذ القانون على الأغراض المبررة بوضوح، مع الاحترام الكامل لمبادئ التناسب والضرورة والقانون المعمول به (مبادئ التناسب والضرورة والقانون الواجب التطبيق). كما يجب أن يتوافق استخدام تقنية التعرف على الوجوه مع متطلبات تقليل البيانات، ودقتها، وتقييد التخزين، وأمن البيانات، والمساءلة (Pajuste, 2021).

3.3 رأي الباحث في استخدام بصمة الوجه الرقمية كنشاط تحقيقي عملي

يرى الباحث بإن واقع استخدام بصمة الوجه الرقمية كنشاط تحقيقي عملي من حيث مدى مشروعيته، يعتمد بدرجة الأساس على مكان إجراء النشاط ومدى التزام القائمين

على تنفيذ إجراءات التحقيق العملي بالضمانات الدستورية، حيث تكفل المادة 37 من الدستور العراقي حرية الفرد العراقي وكرامته، كما تكفل المادة 17 من الدستور العراقي حق الفرد العراقي في الخصوصية بما لا يتعارض مع حقوق الآخرين أو النظام العام أو أي حقوق تمس أمن الدولة الداخلي أو الخارجي(People of Iraq, n.d.)، أذ لا خلاف في إن إجراء النشاط في مكان خاص يعد غير مشروعا، كونه يشكل خرقا دستوريا لحق الفرد في حرمة خصوصياته، حتى ولو كانت واقعة موضوع النشاط يقع تحت طائلة قانون العقوبات، ويساوي في ذلك أن يكون أجهزة أجراء النشاط قد وضعت في المكان الخاص بذاته أو وضعت على بعد في مكان عام ولكنه متوجه لذات المكان الخاص مراقبا له .

بالاستناد إلى قرار البرلمان الأوروبي رقم (INI(2016/2020)) بشأن استخدام الذكاء الاصطناعي في القانون الجنائي ومن قبل الشرطة والسلطات القضائية في المسائل الجنائية، يؤكد الباحث أهمية تضمين مبادئ التناسب والضرورة والقانون النافذ في مشروع قانون جرائم المعلوماتية العراقي، المنتظر إقراره من قبل مجلس النواب العراقي، بوصفها مبادئ دستورية ضامنة للحقوق والحريات الفردية، ومن ثم في اللوائح التنظيمية لاستخدام هذه التقنية. ويأتي ذلك في ضوء المادة (17) من الدستور التي تنص على: "أولاً: لكل فرد الحق في الخصوصية الشخصية بما لا يتعارض مع حقوق الآخرين والآداب العامة. ثانياً: حرمة المساكن مصونة ولا يجوز دخولها أو تفتيشها أو التعرض لها إلا بقرار قضائي ووفقاً للقانون".

4.التحديات التي تواجه الاستخدام المسؤول والخلاق لنتائج تقنية بصمة الوجه الرقمية فيما يتعلق بالخصوصية والحياة الخاصة للأفراد

بشكل عام، حرمة الحياة الخاصة للأفراد بخصوصياتها الطبيعة التي كانت في الماضي محاطة بضلال كثيفة بحيث لا تسمح للغير بالكشف عنها، أصبحت الان بحكم ثورة تكنولوجيا المعلومات غير ذي قبل، أي أصبح بإمكان الافراد والمؤسسات الاطلاع والكشف على حياة الفرد وانشطته الخاصة في ثواني معدودة، خصوصا بعد انتشار بنوك المعلوماتية الخاصة بالدول والمؤسسات وحتى بالأفراد العاديين. ومن هنا بدأت الحاجة الى الحماية الدستورية للخصوصية المتمثلة بالخصوصية المعلوماتية (الخصوصية الرقمية)، درءا للمساس السلبي من قبل أدوات تقنية المعلوماتية للبيانات الشخصية، وعمليا تطلب ذلك التدخل التشريعي لتنظيم أنشطة هذه التقنية من خزن البيانات الشخصية في بنوك وقواعد المعلومات ومعالجتها وتبادلها، على أن يجسد هذا التنظيم الدستوري الطريق الى إقرار قواعد قانونية (جنائية) خاصة يترتب عليها المسؤولية الجنائية في حال مخالفة هذه الانشطة لقواعد التعامل القانوني المسؤول والخلاق مع هذه البيانات الشخصية، أو أي نشاط اخر يتسبب بانتهاك مبادئ الخصوصية الشخصية والحياة الخاصة للأفراد المنظمة دستوريا "Information Privacy Principles Short Guide – Office of the Victorian Information Commissioner," n.d.).

إن النظام الجنائي مقيد بمبدأين دستوريين: مبدأ بطلان الجرائم (لا جريمة ولا عقوبة إلا بنص) ومبدأ الشرعية الجنائية (حظر الاستدلال بالقياس التمثيلي في القانون الموضوعي الجنائي). ولذلك، ولكي يكون نظام العدالة الجنائية فعالاً في المتابعة والتحقيق والمساءلة، فإن قواعد الإجراءات الجنائية في مجالات التحقيق والضبط والمحاكمة يجب أن تحقق التوازن بين حماية الحقوق من جهة وحماية خصوصية الفرد وحياته الخاصة من جهة أخرى. وفي هذا الصدد، ننطلق من ثلاث وجهات نظر دستورية: وجهة النظر اللاتينية، وتسمى الحق في الحياة الخاصة؛ وجهة النظر الأنجلوسكسونية، وتسمى الحق في الخصوصية(Bradford, 2023) ؛ ووجهة النظر الروسية، وتسمى إدارة (مراقبة) الحقوق والحريات.

4.1 المنظور اللاتيني للحق في الحياة الخاصة

بشكل عام يختلف مدلول الحق في الحياة الخاصة في وجهة النظر هذه باختلاف فروع القانون، لذا فمفهوم الحق في الحياة الخاصة في الفرع الجنائي يندرج ضمن قائمة الحقوق الفردية اللصيقة بالفرد، وموضوعه الاساسي يكمن في مايريد الفرد في التستر عليه واخفائه عن علم الغير، ومن ثم الاعتداء على هذا الحق يندرج ضمن فئة الجرائم الحظر، حيث ان هذه الفئة لا تتطلب نتيجة ملموسة. ورغم الاتفاق على وجوب حماية هذا الحق، إلا أن الصعوبة تكمن في تعريفه، أي ماهية الحياة الخاصة. فلا تزال هناك اختلافات كبيرة بين الكتاب الفرنسيين حول وجهات نظرهم في تعريف الحياة الخاصة، إلى حد أن بعض الكتاب يسعون إلى مزيد من الاجتهادات للوصول إلى اتفاق دستوري حول مفهوم الحياة الخاصة(Wagner, 1971) ، رغم وجود اتفاق في الفقه الفرنسي حول المفهوم، عندما يتم تعريفها على أنها عدة دوائر، فإن الدائرة التي تقع في مركزها هي حرمة الحياة الخاصة. ولذلك، فمن المتعارف عليه في هذا المنظور أن مفهوم الحياة الخاصة نفسها له عدة دوائر، تبدأ من النواة التي تشكل نواتها الداخلية، والتي تسمى حرمة الحياة الخاصة. لذا، وبما أن الحرمة جزء من الحياة الخاصة وتشكل النواة الداخلية، أي الجزء الأعمق من الحياة الخاصة، فلا يمكن دراسة الحرمة دون دراسة مفهوم الحياة الخاصة نفسها أولاً.

استنادًا إلى المرسوم رقم 2019-536 الصادر في 29 مايو 2019 عن البرلمان الفرنسي لتطبيق القانون رقم 78-17 المؤرخ في 6 يناير 1978 المتعلق بتكنولوجيا المعلومات والملفات والحريات (والذي يعرف بـ "المرسوم التنفيذي")، أصبح قانون حماية البيانات الفرنسي، بصيغته المعدلة بموجب مرسوم صادر في 12 ديسمبر 2018، نافذًا. وقد ساهم هذا المرسوم في مواءمة القانون الفرنسي مع اللائحة العامة لحماية البيانات للاتحاد الأوروبي The EU General Data Protection Regulation ("GDPR")وتوجيه الشرطة والعدالة الجنائية للاتحاد الأوروبي (التوجيه 680/2016). يوضح المرسوم القواعد الإجرائية لهيئة حماية البيانات الفرنسية، بما في ذلك صلاحياتها وعقوباتها، ويحدد بمزيد من التفصيل حقوق أصحاب البيانات (Hunton Andrews Kurth LLP, 2019).

4.2 المنظور الأنجلوسكسوني للحق في الخصوصية

في الفقه الأنجلوسكسوني، الحق في الخصوصية هو الحق في التمتع بحياة شخصية منعزلة دون علم الآخرين، أو السرية(Kohl, 2023) ، ويعبر عنه بعدة مصطلحات أخرى منها العزلة) الحق في العزلة (The right to isolation - والحق في الانطواء والانزواء (The right to seclusion) والحق في الانفراد والانفصال (The

(The right to individuality and separation)والحق في عدم التدخل (right to noninterference). ومع ذلك، فإن هذا المنظور هو جزء من مفهوم الحق في الخصوصية. ونظراً لارتباط الحق في الخصوصية بالحريات الأساسية في الدستور الأمريكي(.First Amendment," n.d") ، فإن المنظور الأمريكي يرى أن هذا الحق يجب أن يعطى نطاقاً واسعاً من الحرية، وبالتالي يجب ألا يقتصر على العلاقات بين الأفراد أو بين هؤلاء الأفراد والدولة، بل يجب أن يكون الحق في العزلة. وعلى غرار المنظور اللاتيني، فإن المنظور الأنجلوسكسوني لا يقدم أيضاً تعريفاً شاملاً لمفهوم الخصوصية. ولعل أشهر تعريف للحق في الخصوصية هو التعريف الذي أصدره معهد القانون الأمريكي(Lrire & Lrire, 2022) (ALI) ، وهو مؤسسة ذات قيمة فقهية كبيرة في الولايات المتحدة. ويعرّف المعهد انتهاك الحق في الخصوصية على النحو التالي: (فكل شخص ينتهك بصورة جدية وبدون وجه حق، حق شخص اخر في الا تصل اموره واحواله الى علم الغير، والا تكون صورته عرضة لانظار الجمهور، يعتبر مسؤولا أمام المعتدي عليه). في رأي الباحث، لا يزال التعريف الأخير غير دقيق من حيث أنه لا يتناول أصول هذا الحق ولا يوضح قيمته القانونية. وبما أن إعمال الحق في الخصوصية يتطلب الاعتراف بحق الفرد في الاطلاع على المعلومات الخاصة به التي يحتفظ بها الآخرون عنه، فينبغي القول إنه حتى لو كان الآخرون هم سلطات الدولة نفسها، فإن من حقهم معرفة المعلومات السرية الخاصة بهم والتي إذا ما تم افشائها قد تسبب لهم ضرراً. لهذا السبب، فإن مفهوم الحق في الخصوصية نسبي. بعبارة أخرى، ما يعتبر خصوصية في وقت ما قد لا يكون كذلك في وقت آخر. وما يعتبر خصوصية في مكان ما قد لا يكون كذلك في مكان آخر، والعكس صحيح. وبالتالي، ليس من السهل تعريف الحق في الخصوصية بدقة. وذلك لأن الحق في الخصوصية يستند إلى أفكار نسبية تختلف باختلاف العادات والتقاليد والأعراف والتطور المستمر للحياة في مختلف الأزمنة والأمكنة.

4.3 المنظور الروسي لإدارة (مراقبة) الحقوق والحريات

لا يقدم المنظور الروسي، مثل سابقيه اللاتيني والأنجلوسكسوني، تعريفًا واضحًا لمصطلح الحياة الخاصة، ولكن أحكام الدستور الروسي تشمل العلاقات الشخصية والعائلية وغيرها من العلاقات التي لا تتعلق بالأنشطة الرسمية. لذلك، وفقًا للدستور الروسي (المادة 24)(Russia, 1994) ، لا يُسمح بجمع وتخزين ونشر المعلومات المتعلقة بالحياة الخاصة، بما في ذلك الحق في الخصوصية والأسرار الشخصية والعائلية وحماية الشرف والسمعة. ويؤكد ذلك القانون المدني للاتحاد الروسي (الفقرة 1 من المادة 152 من القانون المدني للاتحاد الروسي) (Russian Federation, 1994) الذي يحظر نشر واستخدام صورة المواطن (بما في ذلك صورته العادية أو تسجيلات الفيديو أو الأعمال الفنية التي يتم تصويره فيها).وكخطوة في تطوير الأحكام الدستورية في الاتحاد الروسي، اعتُمد القانون الاتحادي بشأن البيانات الشخصية رقم 152 FZ- المؤرخ 27 تموز/يوليه 2006") سياسة معالجة البيانات الشخصية(.n.d ",، الذي ينظم العلاقات المتعلقة بمعالجة البيانات الشخصية، وأعيد التأكيد على مبادئ وشروط معالجة البيانات الشخصية، وحقوق أصحاب البيانات الشخصية (الأفراد والكيانات القانونية)، وتم إعادة التأكيد على حقوق والتزامات المشاركين الآخرين.

في سياق تعريف الحياة الخاصة، يُعرّف القانون الروسي البيانات الشخصية على أنها أي معلومات تتعلق بشكل مباشر أو غير مباشر بفرد محدد أو يمكن تحديد هويته (صاحب البيانات). ويُقصد بمعالجة البيانات الشخصية أي نشاط (عملية) أو سلسلة من الأنشطة (العمليات) التي تتم باستخدام أدوات آلية أو بدونها") سياسة معالجة البيانات الشخصية، .(n.d. "ويشمل ذلك جمع البيانات الشخصية ومعالجتها وتنظيمها وتخزينها وتوضيحها (تحديثها وتعديلها) واستخراجها واستخدامها ونقلها (توزيعها وتوفيرها والوصول إليها) وإلغاء شخصيتها وحظرها وحذفها وإتلافها. وعلاوة على ذلك، ينص القانون على أنه لا يجوز معالجة المعلومات التي تميز الخصائص الفسيولوجية والبيولوجية التي يمكن أن تحدد هوية الفرد (البيانات الشخصية البيومترية) إلا بموافقة خطية من صاحب البيانات.

4.4 المنظور المقترح من قبل الباحث

باعتبار أن جوهر الخصوصية في العصر الرقمي الحالي، القائم على حق الفرد في خصوصية المعلومات، نعتقد أن أهم غرض للخصوصية بمعناها الواسع: فيما يتعلق بالمعلوماتية (الخصوصية الرقمية)، هو إدارة المعلومات الشخصية والتحكم فيها وهي القدرة على القيام بذلك. من ناحية أخرى، يرى البعض أن الخصوصية في مجال المعلوماتية هي مجرد حق الأفراد في التحكم في عملية جمع المعلومات الشخصية عنهم ومعالجتها وتخزينها وتوزيعها واستخدامها آلياً لاتخاذ القرار والتأثير. ومع ذلك، من وجهة نظرنا، فإن خصوصية المعلومات أمر بالغ الأهمية بالنسبة للحق الأوسع للخصوصية الشخصية فيما يتعلق بقدرة الفرد على أن يقرر بحرية متى وكيف ولأية أغراض تتم معالجة معلوماته الشخصية من قبل الآخرين. لذلك نؤيد أن حماية هذه الخصوصية أمر ضروري لضمان كرامة الأفراد وأمنهم وتقرير مصيرهم بطريقة تسمح لهم بتطوير شخصيتهم بشكل كامل وبحرية. كما أننا نعتقد أن الآثار السلبية المحتملة للمعلوماتية لها تأثير سلبي كبير على مجال الحقوق المتأصلة في الشخصية، والتي يقع الحق في خصوصية المعلومات في صميمها.

من المنظور الذي يقترحه الباحث، سيكون لمبادئ القانون (المبادئ القانونية المقترح تضمينها في مشروع قانون الجرائم الإلكترونية) أثر مرجعي على القاضي، أي أنها ستكون نقطة مرجعية للقاضي في تطبيق القانون. وفي الوقت نفسه، سيكون لآلية هذه المبادئ أثر مستقل على العلاقات العامة، التي ستخضع للتنظيم القانوني العقائدي، أي العقيدة الجنائية الرقمية الذي يخضع له المشرع الجنائي .

في هذا الشأن يقترح الباحث أن يكون العقيدة الجنائية العراقية الرقمية مبنيا على ثلاث مبادئ جوهرية؛ المبدأ الاول: الشرعية: والذي يتمثل في سيادة القانون المعياري والالتزام غير المشروط والدقيق لدستور جمهورية العراق الاتحادي فيما يتعلق بالخصوصية، وبالتالي تنفيذ القاضي لجميع تعليماته. لذا نعتقد بان جوهر هذا المبدأ ينحدر من الفكرة التي يتوسطها الوعي، ويتجسد في فهم وإقناع القاضي بسيادة القانون، والنقطة الاساسية هنا تكمن في الية تنفيذ تحويل شعاريه الافكار الى تنفيذها الالزامي والطبيعي من حيث مراعاة الموجبات، أي التنفيذ الصارم لمتطلبات القانون المعياري والدستور. والمبدأ الثاني:احترام ومراعاة حقوق الإنسان والحريات المدنية: ووفقاً لهذا المبدأ الدستوري، يُحظر جمع وتخزين واستخدام ونشر المعلومات المتعلقة بالحياة الخاصة للفرد دون موافقته. والمبدأ الثالث: يمكن تجسيد مبدأ حماية البيانات من

خلال قيام المشرع العراقي بسن قوانين جديدة لحماية خصوصية المعلومات والبيانات الشخصية من أجل منع إفشاء البيانات الشخصية للأفراد وإساءة استخدامها.

5. الخاتمة

تؤدي بصمة الوجه الرقمية كنشاط تحقيقي عملي دورا مهما في التعرف على الشخصية من خلال كاميرات الرصد والمراقبة، سوآءا كان في مكافحة الجريمة بعد وقوعها أو التنبؤ بوقوعها. ويستنتج الدراسة بإن اجراء هذا النشاط الوقائي من قبل الأجهزة الامنية في مجال الضبط الاداري لابد وأن يكون مقترنا بالإعلان عن المنطقة المراقبة في المكان العام، وعدم تركيز الكاميرات على الافراد بشكل خاص الا إذا كان هناك مبرر يستدعي ذلك مع مراعاة شرط توفير الضمانات الدستورية بدقة. كما ويستنتج الدراسة بان بصمة الوجه الرقمية كنشاط تحقيقي عملي ينبغي الاخذ بها على شكل دليل جنائي في الاجراءات الجنائية العراقية ومن دون الحاجة الى استصدار إذن قضائي بذلك، متى ما كان المكان عاما ومراعيا للضمانات الدستورية، على اعتبار بصمة الوجه الرقمية من حيث ظروف وملابسات قبولها خاضع الى السلطة التقديرية للقاضي الجنائي، وبالتالي يخضع هذا النشاط كسائر الأدلة الجنائية الاخرى الى مبدأ مشروعية الدليل الجنائي. وفي النهاية، توصي الدراسة المشرع الجنائي العراقي بأن يتدخل مرة أخرى ويعدل مشروع قانون جرائم المعلوماتية، بحيث يشمل على الضمانات اللازمة الثي تكفل عدم التعدي على حرمة وسرية الحياة الخاصة للأفراد، وبالتالي عدم اعتبار بصمة الوجه الرقمية كنتيجة تلقائية للنشاط التحقيقي العملي في اعتباره دليل جنائي حتمي يعتدي به قضائيا، ما لم يكن متوافقا مع الضمانات الدستورية الكفيلة بذلك، وهذه الضمانات تخضع لرقابة الادعاء العام والاشراف القضائي.

المراجع

Abudarham, N., Grosbard, I., & Yovel, G. (2021). Face Recognition Depends on Specialized Mechanisms Tuned to View-Invariant Facial Features: Insights from Deep Neural Networks Optimized for Face or Object Recognition. Cognitive Science, 45(9). https://doi.org/10.1111/cogs.13031

Allyn, B. (2020, June 24). "The Computer Got It Wrong": How Facial Recognition Led To False Arrest Of Black Man. NPR. https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig

Berle, I. (2020). Face Recognition Technology. In Law, governance and technology series. https://doi.org/10.1007/978-3-030-36887-6

Bradford, A. (2023). Digital empires: The Global Battle to Regulate Technology. Oxford University Press.

Crawford, K. (2019). Halt the use of facial-recognition technology until it is regulated. Nature, 572(7771), 565. https://doi.org/10.1038/d41586-019-02514-7

First Amendment. (n.d.). Retrieved from https://www.law.cornell.edu/wex/first_amendment#:~:text=It%20enforces%20the%20%22separation%20of,the%2

0content%20of%20the%20speech.

Michalski, D., Malec, C., Clothier, E., & Bassed, R. (2024). Facial recognition for disaster victim identification. Forensic Science International, 361, 112108. https://doi.org/10.1016/j.forsciint.2024.112108

Dessimoz, D., & Champod, C. (2015). A dedicated framework for weak biometrics in forensic science for investigation and intelligence purposes: The case of facial information. Security Journal, 29(4), 603–617. https://doi.org/10.1057/sj.2015.32

State Duma. (1995). Federal Law No. 144-fz Of August 12, 1995 on Operational-search Activities. In Russian Federation [legal Document]. Https://www.wto.org/english/thewto_e/acc_e/rus_e/wtaccrus58_leg_373.pdf

Lois, C., & Groves, J. O. (2011). Genetics in non-genetic model systems. Current Opinion in Neurobiology, 22(1), 79–85. https://doi.org/10.1016/j.conb.2011.11.002

Lrire, & Lrire. (2022, April 10). ALI Data Privacy: Overview and Black Letter text. Retrieved from https://www.uclalawreview.org/ali-data-privacy-overview-and-black-letter-text/

People of Iraq. (n.d.). Constitution of Iraq. https://iq.parliament.iq/en/wp-content/uploads/sites/3/2024/04/Constitution-of-the-Republic-of-Iraq.pdf

Al-Shehri, A. M. Z. & Department of Jurisprudence - Majoring in Regulations - College of Sharia and Fundamentals of Religion - King Khalid University - Saudi Arabia. (2022). The authoritativeness of the digital evidence in the Saudi system and Islamic jurisprudence. https://fica.journals.ekb.eg/article_309970_d40e911937ee4fd151d8126279e489c7.pdf

Khoo, L. S., & Mahmood, M. S. (2020). Application of facial recognition technology on identification of the dead during large scale disasters. Forensic Science International Synergy, 2, 238–239. https://doi.org/10.1016/j.fsisyn.2020.07.001

Kohl, U. (2023). The Right To Be Forgotten In Data Protection Law And Two Western Cultures Of Privacy. International And Comparative Law Quarterly, 72(3), 737–769. Https://doi.org/10.1017/s0020589323000258

Choung, H., David, P., & Ling, T. (2024). Acceptance of AI-Powered Facial Recognition Technology in Surveillance Scenarios: Role of Trust, Security, and Privacy Perceptions. Technology in Society, 102721. https://doi.org/10.1016/j.techsoc.2024.102721

Lai, X., & Rau, P. P. (2021). Has facial recognition technology been misused? A public perception model of facial recognition scenarios. Computers in Human Behavior, 124, 106894. https://doi.org/10.1016/j.chb.2021.106894

Yu, Z., Zhou, Y., Mao, K., Pang, B., Wang, K., Jin, T., Zheng, H., Zhai, H., Wang, Y., Xu, X., Liu, H., Wang, Y., & Han, J. J. (2024). Thermal facial image analyses reveal quantitative hallmarks of aging and metabolic diseases. Cell Metabolism, 36(7), 1482-1493.e7.

12.08.1995 N 144-FZ (poslednjaja redakcija) \ Konsul'tantPljus. (n.d.). Retrieved from https://www.consultant.ru/document/cons_doc_LAW_7519/

. (n.d.). Retrieved from سياسة معالجة البيانات الشخصية https://halaltravelrussia.com/politika-obrabotki-personalnyh-dannyh/

Abstract:
Facial recognition technology (FRT), an application of artificial intelligence algorithms using surveillance cameras and contemporary technology, functions as digital evidence in algorithmic criminology. FRT captures facial characteristics such as ears, mouth, eyes, chin, and cheeks, which are then treated as conventional scientific evidence in criminal investigations. Its current applications include identity verification at border crossings, airports, and ATMs. The study examines FRT's problematic application in contemporary criminal proceedings, particularly in criminal evidence, using descriptive and analytical approaches to highlight its relevance. The research aims to legally understand FRT and demonstrate its importance as an operational investigative activity in modern criminal proceedings, reviewing arguments for and against its use. The study found FRT plays a significant role in criminal evidence and has a preventive function in administrative control. Recommendations include ensuring the legitimacy of FRT's purpose and methods, usage in public spaces, and consideration of individual privacy rights. Furthermore, the study stresses the necessity of digital and technical training for judicial and investigative officers through specialized courses bridging legal science and digital technology. The study recommends amending the Iraqi draft cybercrime law to include safeguards protecting individuals' privacy. It asserts that facial recognition technology in investigations must align with constitutional guarantees overseen by public prosecution and judicial supervision.
Keywords: Facial Recognition Technology, combating crime, Operational Investigative Activity, Contemporary Criminal Proceedings, Digital Evidence, Iraqi Cybercrime Law.

https://doi.org/10.1016/j.cmet.2024.05.012

Johnson, T. L., Johnson, N. N., McCurdy, D., & Olajide, M. S. (2022). Facial recognition systems in policing and racial disparities in arrests. Government Information Quarterly, 39(4), 101753. https://doi.org/10.1016/j.giq.2022.101753

Johnson, T. L., Johnson, N. N., Topalli, V., McCurdy, D., & Wallace, A. (2024). Police facial recognition applications and violent crime control in U.S. cities. Cities, 155, 105472. https://doi.org/10.1016/j.cities.2024.105472

Hunton Andrews Kurth LLP. (2019, June 13). New French Data Protection Act and implementing decree take force. Retrieved from https://www.hunton.com/privacy-and-information-security-law/new-french-data-protection-act-and-implementing-decree-take-force

Russia. (1994). Constitution of the Russian Federation: With Commentaries and Interpretation. Brunswick Publishing Corp.

Russian Federation. (1994). The Civil Code Of The Russian Federation. Retrieved From Https://www.wto.org/english/thewto_e/acc_e/rus_e/wtaccrus58_leg_360.pdf

Information Privacy Principles Short Guide – Office of the Victorian Information Commissioner. (n.d.). Retrieved from https://ovic.vic.gov.au/privacy/resources-for-organisations/information-privacy-principles-short-guide/

Tripathi, B. K. (2017). On the complex domain deep machine learning for face recognition. Applied Intelligence, 47(2), 382–396. https://doi.org/10.1007/s10489-017-0902-7

Pajuste, T. (2021). Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters - Wednesday, 6 October 2021. (n.d.). Retrieved from https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html

Wagner, W. J. (1971). The development of the theory of the right to privacy in France.

Sajta, A. (n.d.). Opublikovan sbornik po itogam konferencii «Enisejskie politiko-pravovye chtenija – 2024». Retrieved from https://lav.sfu-kras.ru/scince/konf/enisejskie-politiko-pravovye-chtenija/opublikovan-sbornik-po-itogam-konferentsii-enisejskie-politiko-pravovye-chtenija-2024

Federal'nyj zakon “Ob operativno-rozysknoj dejatel'nosti” ot