IRAQI Academic Scientific Journals
العراقية المجلات الأكاديمية العلمية
مجلة جامعة الكوت للعلوم الإنسانية
ISSN (E): 2707 – 5648 II ISSN (P): 2707 – 563 x
jh.uokut.edu.iq
k.u.c.j.hum@alkutcollege.edu.iq
المجلد 7 ، العدد 1 ، حزيران 2026

المسؤولية الجنائية عن التلاعب بأنظمة البصمة الالكترونية (دراسة مقارنة)

م. م. حواء علي إبراهيم الأسدي [1]

المستخلص

شهد العالم في العقود الأخيرة تطوراً هائلاً في وسائل التقنية الحديثة، كان من أبرزها اعتماد أنظمة البصمة الإلكترونية كوسيلة لإثبات الهوية والتحقق من شخصية الأفراد في مجالات متعددة، مثل المؤسسات الحكومية والمصارف والشركات وحتى المؤسسات التعليمية، وتمثل هذه الوسائل نقلة نوعية في تعزيز الدقة والسرعة ومنع التلاعب بالبيانات الشخصية، غير أن هذا التطور لم يَخْلُ من مخاطر، إذ ظهرت صور متعددة للتلاعب بتلك الأنظمة، سواء عبر تزوير البصمة أو انتحال هوية الغير أو اختراق الأنظمة الإلكترونية، مما يثير إشكاليات قانونية وجنائية خطيرة تتعلق بحماية الثقة العامة وضمان سلامة التعاملات.

الكلمات المفتاحية: مسؤولية، تلاعب، انظمة، بصمة، الكترونية

انتساب الباحث
[1] كلية القانون، جامعة الكوت، العراق، واسط، الكوت، 52001

[1] hawaassdi@gmail.com

[1] **المؤلف المراسل**

معلومات البحث
تأريخ النشر : حزيران 2026

Criminal liability for Tampering with Electronic Fingerprint Systems (a Comparative Study)

Hawa Ali Ibrahim Al-asadi [1]

Abstract

In recent decades، the world has witnessed tremendous advancements in modern technology، most notably the adoption of electronic fingerprint systems as a means of identity verification and authentication in various sectors، including government institutions، banks، companies، and even educational establishments. These systems represent a qualitative leap in enhancing accuracy and speed while preventing the manipulation of personal data. However، this development has not been without its risks. Various forms of manipulation of these systems have emerged، including fingerprint forgery، identity theft، and hacking، raising serious legal and criminal issues related to protecting public trust and ensuring the integrity of transactions.

Keywords: Responsibility، manipulation، systems، fingerprint، electronic

Affiliation of Author
[1] College of Law, University of Kut, Iraq, wasit, Kut, 52001

[1] hawaassdi@gmail.com

[1] **Corresponding Author**

Paper Info.
Published: Jun. 2026

المقدمة

شهد العالم خلال العقدين الأخيرين تحولًا رقميًا واسعًا اعتمدت فيه المؤسسات الحكومية والخاصة على الأنظمة البيومترية في إدارة الهوية والتحقق من الشخصية، ومنها أنظمة البصمة الإلكترونية التي أصبحت وسيلة أساسية في ضبط الحضور والانصراف، وتأمين الدخول إلى الأنظمة، وتوثيق المعاملات الرسمية.

فقد بدأت عدة مؤسسات وإدارات باستخدام نظام البصمة الالكترونية، إذ جاءت فلسفة البصمة الالكترونية بهدف ضبط الدوام، ويتميز هذا النظام بأنه يعطي مرونة عالية في إصدار تقارير تراكمية لحركة العاملين في مجال (الحضور، والغياب، ومغادرة، وتأخر المهمات الرسمية)، وذلك على مستوى الإدارات، ويعدّ هذا التطبيق نوعا من استخدام نظام الرقابة الالكترونية، الأمر الذي يوجب على الموظفين والعمال الالتزام التام بالدوام.

ومن استخدامات البصمة الالكترونية تكوين قواعد البيانات البيومترية، وهي قاعدة بيانات محوسبة تُجمَع فيها بيانات شخصية تشمل البصمات وملامح الوجه لكل شخص، وهي المستخدمة في بعض أنظمة الشركات، وإدارة الحضور والانصراف، وتسجيل بصمة الفرد، لتُدرَج ضمن بقية بياناته الشخصية، إذ إن البصمة الالكترونية توفر سرعة كبيرة في التميز بين البصمات.

وقد أصبح من الممكن أيضًا التعرّف على الشخص، فقد تكفّلت البصمة بحفظ الهوية الشخصية عِبر تفعيلها في المديريات، والأحوال المدنية، والجوازات، فضلاً عن بعض الدوائر الحكومية الأخرى وقننت أنظمة الحضور والغيابات من خلال تفعيل نظام البصمة الذي جاء عوضا عن التوقيع الكتابي للحضور والانصراف (كشف الدوام الرسمي) لتحديد وقت والانصراف تجنبا للوقوع في كثير من الأخطاء ومشكلات التلاعب.

مع هذا التطور التقني برزت تحديات جديدة تتعلق بمحاولات بعضهم التحايل على هذه الأنظمة أو اختراقها أو التلاعب ببياناتها، الأمر الذي خلق نمطًا حديثًا من الجرائم الإلكترونية يُعرف بـ جريمة التلاعب بأنظمة البصمة الإلكترونية.

تتمثل هذه الجريمة في كل سلوك يهدف إلى تزوير أو استبدال أو تعطيل أو تغيير بيانات البصمة الإلكترونية أو الأجهزة والبرمجيات التي تعتمدها، بقصد الحصول على منفعة غير مشروعة أو الإضرار بغيره أو إخفاء حقيقة واقعية.

وتُعد من الجرائم الخطرة لأنها تمس ثقة الدولة والمؤسسات في أدوات التحقق من الهوية، كما تهدد سرية البيانات الشخصية وتفتح الباب أمام جرائم أكبر مثل الاختراق، وانتحال الصفة، والاستيلاء على المال العام أو الخاص.

أولاً- أهمية البحث

بيان مدى كفاية النصوص التشريعية العراقية في مواجهة هذا النمط المستحدث من الجرائم، فضلاً عن مقارنته ببعض التشريعات العربية، للوصول إلى حلول تشريعية عملية.

ثانياً- أهداف البحث

1. بيان الطبيعة القانونية لأنظمة البصمة الإلكترونية ومجالات استخدامها.
2. تحديد صور التلاعب بتلك الأنظمة وطرق ارتكابها.
3. تكييف الأفعال المرتكبة وفق القانون الجنائي العراقي.
4. مقارنة موقف القانون العراقي بالقانون المصري

ثالثاً- إشكالية البحث

إلى أي مدى يسعف القانون الجنائي العراقي في مواجهة جريمة التلاعب بأنظمة البصمة الإلكترونية، وما الموقف في التشريعات المقارنة؟

رابعاً- منهجية البحث

ركز هذا البحث على أهم المناهج الآتية:

1. المنهج التحليلي إذ يقوم على استعراض النصوص القانونية التي تعالج موضوع البحث.
2. المنهج الاستقرائي وذلك عن طريق استعراض الجزيئات الدقيقة للجريمة.
3. المنهج المقارن لكل من القانون العراقي والقانون المصري إذ اعتمدنا مقارنة النصوص العقابية المتعلقة بموضوع بحثنا.

خامساً- هيكلية البحث

المبحث الأول: مفهوم أنظمة البصمة الإلكترونية.

المطلب الأول: تعريف البصمة الإلكترونية.

المطلب الثاني: صور التلاعب بأنظمة البصمة الإلكترونية.

المطلب الثالث: ذاتية البصمة الالكترونية.

المبحث الثاني: المسؤولية الجنائية عن التلاعب بأنظمة البصمة الإلكترونية.

المطلب الأول: أركان جريمة التلاعب بأنظمة البصمة الإلكترونية.

المطلب الثاني: المسؤولية الجنائية للموظف أو مكلف بخدمة عامة عن التلاعب بأنظمة البصمة الإلكترونية.

المطلب الثالث: التكييف القانوني للتلاعب بأنظمة البصمة الإلكترونية والعقوبة المترتبة عليها.

الخاتمة

المبحث الأول

مفهوم أنظمة البصمة الإلكترونية

نالت البصمة اهتمامًا بالغًا من المختصين والعلماء والباحثين وقد تعددت التعريفات بشأنها، أما انظمة البصمة الإلكترونية هي تقنيات حديثة تُستخدم للتحقق من الهوية عبر الخصائص الحيوية للأفراد [1]، لضمان الدقة والأمان في المعاملات والإجراءات، وقُسمَ هذا المبحث على ثلاثة مطالب:

المطلب الأول

تعريف البصمة الإلكترونية

سنوضح في هذا المطلب تعريف البصمة الإلكترونية لغةً واصطلاحاً في كل من التشريع العراقي والمصري على النحو الآتي:

أولاً: البصمة لغةً.

أَثر الختم بالإصبع [2]، بَصَمات: خَتْم: «بَصْمة صاحِب مَصْنع «أَثَر الوَطْء الَّذي تَتْركُه قَدَمُ الحَيَوان: «بَصْمة حافِر حِصان» أَثَر، علامة، دَمْغة «بَصْمةُ خاتم»، بَصْمةُ قُماش، أَثَرَ الختم بالإصبع: "ترك بَصَمات أَصابعه على باب الخزانة" [3]، صورة من

النتوءات والانحناءات المسامية في جلد أطراف الأصابع؛ أثر هذه النتوءات في شيء، علامة يطبعها إفراز مادة دهنية؛ تُستخدم دليلاً قاطعاً في تحقيق الشخصية [4].

البصمة مشتقة من البصم وهي أثر ختم الاصبع، فهو ذلك الخاتم الإلهي الذي ميز الله سبحانه وتعالى به كل انسان عن غيره، كبصمة الصوت، والعين، والرائحة، والاذن، وغيرها من البصمات التي لا تتشابه أو تتماثل مع أي شخص في الكون [5].

البصم كلمة عربية اصيلة تعني الفارق بين الاصبعين: الخنصر والبنصر، أو تعني الغلظة والكثافة وقد نتج عنها معنى جديد اقر به نخبة من ادباء اللغة العربية في مصر وهو: أثر الختم بطرف الأصبع بعد دهنه بمادة خاصة بذلك، وهي في مكوناتها تشبه المداد الأسود، وهي من اجل ان تترك أثر أو ما يسمى بالطبعات التي تظهر بعد وضع البنان على المداد مثلا، ثم يتم لمس سطح أملس أو أي ورق فتطبع عليه آثاره، وهو ما يطلق عليه البصمة [6].

ثانياً: البصمة الالكترونية اصطلاحاً:

عن طريق دراستنا نرى غياب تعريف صريح في قانون العقوبات العراقي، إذ لا يحتوي على تعريف مباشر لـ "البصمة الإلكترونية"، ولم يتناول الجرائم الإلكترونية ضمن قوانينه [7]، ويمكن تعريف البصمة بأنها الآثار أو العلامات أو الطبعات التي تتركها رؤوس الأصابع وراحة اليد والأقدام بعد ملامسة الأسطح المصقولة، لأن الأسطح الخشنة يصعب رفع البصمات من فوقها بسبب التعرجات والتجاويف التي تكون فيها [8].

بالعودة الى مشروع قانون مكافحة الجرائم المعلوماتية العراقي لسنة ٢٠١٩نجده يوضح في المادة الاولى منه، الفقرة اولا، بأنها" كل فعل يرتكب باستخدام الحاسب الالي او شبكة المعلومات او غير ذلك من وسائل تقنية المعلومات المعاقب عليها وفقًا لأحكام القانون [9].

بذلك تُعد البصمة الإلكترونية وسيلة لـإثبات الحضور والانصراف باستخدام الخصائص البيومترية للفرد، كالخطوط الفريدة لبصمة الإصبع، وتحويلها إلى بيانات رقمية تُخزن وتُستخدم للتحقق من هوية الشخص [10]، كذلك يمكن ذكر "البيانات البيومترية" (Biometric Data) أية بيانات رقمية ناتجة عن قياسات بيولوجية أو خصائص فيزيائية تُستخدم للتحقق من هوية الشخص، وهذه تشمل البصمة الإلكترونية بشكل صريح [11].

إما القانون المصري من الدول العربية التي نصّت بشكل واضح على البيانات الحيوية البيو مترية في تشريعاتها، ومنها: قانون حماية البيانات الشخصية المصري [12]، بقولها "البيانات الشخصية أيَة بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأيَة بيانات أخرى كالاسم، أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية"، "والبيانات الشخصية الحساسة: البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية، أو بيانات القياسات الحيوية "البيو مترية" أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية أو الحالة الأمنية، وفي جميع الأحوال تعد بيانات الأطفال من البيانات الشخصية الحساسة" [13].

من خلال اطلاعنا على القرارات القضائية لم نجد القضاء يورد تعريفاً للبصمة الإلكترونية ولكن وضحها بعض فقهاء القانون بقولهم، "نظام يعتمد على الخصائص الحيوية للشخص لتوليد شفرة رقمية تُستخدم كوسيلة لإثبات الهوية في الأنظمة الإدارية أو الأمنية" [14].

كذلك عُرّفت أنظمة البصمة الإلكترونية بأنها أنظمة تقنية تعتمد الخصائص البيومترية الفريدة للإنسان للتحقق من الهوية، مثل بصمة الإصبع، والوجه، والعين، والصوت، أو التوقيع. وتُعد هذه الأنظمة وسيلة حديثة لإثبات الشخصية بدقة عالية، وتُستخدم على نطاق واسع في المؤسسات الحكومية، الأمنية، التعليمية، والمصرفية [15].

يمكن للباحثة صياغة تعريف للبصمة الإلكترونية بأنها (كل بيانات بيومترية رقمية تُسجَّل أو تُعالَج بواسطة أنظمة إلكترونية بهدف التحقق من هوية الشخص، وتشمل بصمة الإصبع، وبصمة الوجه، وبصمة العين، أو أي نمط بيومتري آخر).

المطلب الثاني

صور التلاعب بأنظمة البصمة الالكترونية

البيانات البيومترية هي خصائص جسدية أو سلوكية فريدة تُستخدم لتحديد الهوية والتحقق [16]، وقد ازدادت أهمية هذه التقنية في قطاعات مختلفة، إذ تُعزز الأمن وتُحسّن تجربة المستخدم، وهناك أنواع مختلفة من الخصائص البيو مترية، بما في ذلك السمات الفسيولوجية مثل التعرف على الوجه [17].

فضلاً عن السمات السلوكية مثل أنماط الصوت، وتشمل القياسات الحيوية قياس الخصائص الجسدية أو السلوكية الفريدة للأشخاص وتحليلها إحصائيًا، وتُستخدم هذه التقنية لتحديد الهوية والتحكم في الوصول إلى البيانات [18]، تُحلل الأنظمة البيو مترية مختلف السمات البيولوجية أو أنماط السلوك لتمييز شخص عن آخر [19]، وتتبع موثوقية البيانات البيو مترية من التباين الطبيعي في السمات، مثل بصمات الأصابع أو تراكيب الوجه [20]، والتي يصعب عادةً تقليدها أو تزويرها مقارنةً بأساليب التعريف التقليدية مثل كلمات

المرور أو بطاقات الهوية [21].

هناك أنواع وصور متعددة للتلاعب بأنظمة البصمة الالكترونية سنبينها على نحو الآتي:

أولاً: أنواع المعرفات البيو مترية.

1. التعرف على الوجه: باستخدام ملامح الوجه، تُحلل هذه التقنية شكل الوجه، والمسافة بين الملامح، وهندسة الوجه العامة، ومع تطور الذكاء الاصطناعي أصبحت أنظمة التعرف على الوجه أكثر تطورًا، مما يوفر دقة أكبر في تحديد هوية الأفراد [22].
2. مسح الشبكية والقزحية: تتضمن هذه الطرق تحليل الأنماط الفريدة في شبكية العين أو قزحيتها، تتميز هذه السمات بدقة عالية، ويصعب تكرارها والبصمة اكتشفتها شركات طبية بعد بحوث طويلة، وتؤكد أنه لا يوجد شخصان متماثلان في بصمة العين إذ يتم أخذ بصمة العين عن طريق جهاز فحص لذلك، يلتقط صورة لشبكية العين، وعند الاشتباه في أي شخص يتم الضغط على زر معين في الجهاز فتتم مقارنة صورته بالصورة المختزنة في ذاكرة الجهاز، ولا يزيد وقت هذه العملية عن ثانية ونصف فقط " ويطلق على هذه العملية أو التقنية " المسح الحدقي " فهي عملية تبين من خلالها المميزات الخاصة بحدقة كل إنسان من أجل التعرف على شخصيته، إذ تبدأ الخطوات بتصوير العين بالفيديو ثم تحويل ما يقرب من 266 ميزة خاصة بالحدقة من بقع وهلالات ودوائر وتجاويف وغيرها إلى شفرة رقمية [23].
3. بصمة الاذن والشعر: عندما يولد الإنسان وينمو ويكبر يتغير في كل شيء إلا بصمة إذنه، فهي البصمة الوحيدة التي لا يعتريها التغير منذ ولادته وحتى إعلان وفاته وكان علماء الانجليز قد طوروا نظام كمبيوتر يسمح بالتعرف على بصمة الأذن بكل يسر وسهولة، أما بصمة الشعر فهي من العناصر الفعالة في عمل البصمة الوراثية، كما أنها تميز الإنسان بدون عمل البصمة الوراثية إذ يعد الشعر من الأدلة الوراثية القوية، سيما أنه لا يتعرض الى التلف مع الوقت، فيمكن من خلال الشعر التعرف على هوية شخصية الضحية أو له بصمة خاصة به لا يمكن أن تتشابه عند أي شخص أخر، وقد أخذت أول بصمة شعر في عام 1950 [24].
4. التعرف على الصوت: تفحص هذه التقنية الأنماط الصوتية، يتميز صوت كل شخص بخصائص مميزة بما في ذلك النبرة والطبقة والإيقاع، مما يجعلها وسيلة فعّالة للتحقق، اكدت الدراسات الحديثة على أنه لكل صوت صفات عضوية فيزيولوجية وهي الصفات التشريحية لمجرى الصوت المتمثلة في حجم الرئتين الحنجرة وطول مجرى الصوت والاوتار الصوتية وسمكها، وغيرها من الصفات الثابتة التي لا يستطيع صاحبها السيطرة عليها، فضلاً عن الصفات المكتسبة الناشئة عن العادات الكلامية للفرد [25].
5. البصمة الوراثية: عرفت البصمة الوراثية أو بصمة الحمض النووي إنها إحدى وسائل التعرف على الشخص عن طريق مقارنة مقاطع من الحمض النووي الريبوزي منقوص الأكسجين وهي المادة الوراثية الموجودة في خلايا جميع الكائنات الحية، وهي التي تجعل كل شخص مختلفًا عن غيره وتعد البصمة الوراثية أصل كل العلامات الوراثية الموجودة بالجنين منذ بداية تكوينه والمسؤولة عن تحديد فصيلة الدم ونوع البروتين والإنزيمات وشكل بصمات الأصابع، وإذا حدث أي خلل فيها ينعكس ذلك على الإنسان في شكل مرض [26].
6. التعرف على بصمات الأصابع: تُعد هذه من أكثر الطرق البيو مترية استخدامًا، بصمات الأصابع فريدة لكل فرد، وأنماطها ثابتة مع مرور الوقت، مما يجعلها وسيلة موثوقة لتحديد الهوية، ويتبين أهمية التعرف على بصمات الأصابع بانها خطوط بارزة في بشرة الجلد تجاورها منخفضات، وتعلو الخطوط البارزة فتحات للمسام العرقية ، تتمادى هذه الخطوط وتتلوى وتتفرع منها فروع لتأخذ في النهاية – وفي كل شخص- شكلا مميزا ، وقد ثبت أنه لا يمكن للبصمة أن تتطابق وتتماثل عند شخصين في العالم حتى التوائم المتماثلة التي أصلها في بويضة واحدة، وهذه الخطوط تترك أثرها على كل جسم تلمسه وعلى الأسطح الملساء بشكل خاص [27].
7. بصمة الرائحة: قال تعالى في محكم كتابه ﴿وَلَمَّا فَصَلَتِ الْعِيرُ قَالَ أَبُوهُمْ إِنِّي لَأَجِدُ رِيحَ يُوسُفَ ۖ لَوْلَا أَن تُفَنِّدُونِ﴾ [28]، فمن خلال هذه الآية الكريمة نجد أنها تؤكد أن هناك بصمة للرائحة من الأدلة القطعية للتعرف على شخص ما، ويمكن اكتشاف تلك البصمة من خلال استغلال كلاب الولف التي تستطيع شم ملابس انسان معين [29].
8. بصمة الشفاه: ويقصد ببصمة الشفاه تلك العضلات الموجودة على الشفاه، وقد ثبت أن بصمة الشفاه صفة مميزة جدا حتى أنه لا يتشابه فيها شخصان في العالم، وتؤخذ بصمة الشفاه بواسطة جهاز به حبر غير مرئي حيث يوضع الجهاز على شفه الشخص المطلوب وقد أجريت تجارب عن بصمة الشفاه في اليابان على مجموعة تحتوي على 364 فردًا من الذكور والإناث ووجود اختلاف بين بصمات الشفاه حتى بين التوائم، وأن بصمات الشفاه لا تتغير مع تقدم السن وأشار البحث إلى

أن بصمات الشفاه لها أهمية بصمات الأصابع نفسها [30].

ثانياً: صور التلاعب فيتضمن ما يأتي.

1. الدخول غير المصرح به عبر البصمة، مثل: استخدام بصمة موظف آخر لتسجيل حضوره أو فتح جهاز أو نظام باستخدام بصمة شخص بطريقة غير قانونية [31].
2. تزوير أو استنساخ البصمة الإلكترونية، مثل: نسخ بصمة إصبع باستخدام جهاز خاص أو استخدام مجسّم لبصمة شخص آخر لفتح نظام حضور باب إلكتروني أو إنشاء بصمة رقمية مزيفة بأحد برامج التعديل.
3. تعديل بيانات البصمة في الأنظمة، مثل: تغيير وقت الحضور والانصراف في جهاز البصمة أو مسح بصمة موظف أو إضافتها دون جهة اختصاص [32].
4. تعطيل أو إتلاف أجهزة نظام البصمة، مثل: تخريب جهاز البصمة لإخفاء الأدلة أو تعطيل نظام الدوام [33].

المطلب الثالث

ذاتية البصمة الالكترونية

أثبتت مجموعة من الدراسات التاريخية القديمة من لجوء الفراعنة المصريين والصينيين والإغريق الى الحصول على بصمة طرفي التعامل كوسيلة لإثبات شخصيتهم وعنهم أخذت هذه العادة الحضارة الأشورية بل أن الباحث الألماني (هندل) أشار في بحوثه أَنهم استخدموا البصمة كوسيلة للبحث والتحري وتعقب ارمين من خلال المقارنة البسيطة لحجم وشكل البصمة [34].

بدأ الاهتمام الحديث للبصمات الأصابع ينحو إلى اتجاه إيجابي من خلال جهود العلماء المحدثين منذ الحقبة الأخيرة من القرن الثامن عشر وحتى وقتنا الحاضر، فقد شهد النصف الثامن القرن الماضي ما يعرف بالثورة الالكترونية التي كان من أهم نتائجها اختراع الحاسبات الآلية والتي تطورت تطورا سريعا أسفر عن زيادة مذهلة في حجم ما تستوعبه وحدة التخزين من بيانات، والوصول إلى سرعات رهيبة في معالجة هذه البيانات والربط بينها واستخلاص مؤشراً وإظهارها في صورة بيانات مكتوبة في وقت زمني قصير وبصورة مكن العلماء من مستخدمي هذه الحاسبات من معالجة الكثير من المشكلات الإنسانية والتي كان علاجها يحتاج إلى جهد بشري [35].

تتضمن ذاتية البصمة الالكترونية في بيان أوجه الشبه والاختلاف بين البصمة الالكترونية وأنواع البصمات التقليدية الأخرى وايضاً يشمل الخصائص التي يمتاز بها البصمة الالكترونية، وسنوضح ذلك على نحو الآتي:

أولاً: خصائص البصمة الالكترونية.

أصبحت غالبية المؤسسات الحكومية وغير الحكومية تطبق نظام البصمة الالكترونية لضبط مواعيد حضور وانصراف موظفيها، وعلى الرغم من إيجابيات هذه الآلية التي عدها البعض أداة مهمة في عملية التقييم ومنح العلاوات، إلا أن بعض الأفراد رفض مقياسا لأداء الموظف، فالحضور في الوقت المحدد والجلوس خلف المكتب لحين انتهاء ساعات الدوام الرسمي، روتين ينتج عنه في كثير من الأحيان موظفون محبطون [36]، وتشمل الخصائص ما يأتي:

1. التفرد (Uniqueness): لا تتطابق بصمات شخصين بنفس البصمة، حتى بين التوائم المتطابقة.
2. الثبات (Permanence): تبقى البصمة ثابتة نسبيًا عبر الزمن، مما يوفر مصادقة مستمرة.
3. سهولة الاستخدام: توفر تجربة دخول سلسة وسريعة مقارنة بكتابة كلمات المرور الطويلة.
4. الدمج: يمكن دمجها مع طرق أخرى (مثل كلمة المرور) لمزيد من الأمان [37].
5. المرونة: يتميز هذا النظام انه يعطي مرونة عالية في إصدار تقارير تراكمية لحركة العاملين في مجال (الحضور، والغياب، والمغادرة، والتأخر، والمهمة الرسمية).
6. الرقابة: يعد هذا التطبيق نوعا من استخدام نظام الرقابة الالكترونية [38].

بذلك نرى ان نظام البصمة الالكترونية يعد الوسيلة المهمة لضبط مواعيد حضور وانصراف الموظفين في الشركات والمؤسسات العامة والخاصة، ومنع جرائم انتحال الشخصية، واختصار الإجراءات، وإنجاز المعاملات بسرعة فائقة.

ثانياً: تمييز البصمة الالكترونية عن البصمة التقليدية.

يعتمد إظهار البصمة التقليدية على طباعتها بالحبر وهو أمر يترك أثراً نفسياً عند الأفراد لكونه مرتبطاً بالتعامل مع المتهمين والمجرمين، كما تعتمد جودة صورة البصمة على مدى خبرة الشخص المشرف على طباعتها ما يفتح المجال واسعاً لوقوع أخطاء شخصية [39].

يستغرق الحصول على النتيجة النهائية في البصمة التقليدية ما بين 24 إلى 48 ساعة عدا عن أن عوامل الدقة تصبح منخفضة نسبياً إذ تجمع بطاقات البصمات وتنقل معاً إلى كمبيوتر البصمات لإجراء عملية البحث والمقارنة، وقد تفقد بعض البطاقات أو تسقط سهواً أو

تستبدل بطاقة بأخرى [40].

أما في البصمة الإلكترونية فيتم إنجاز جميع المراحل عبر نظام آلي دقيق جداً ومبرمج سلفاً وتكاد تكون فيه نسبة الأخطاء بسيطة للغاية، ما جعل البصمة الإلكترونية من الأنظمة المعتمدة حالياً في أكثر الدول تقدماً مثل أمريكا وبريطانيا وأستراليا والإمارات وغيرها تبعاً لإمكانات كل دولة نظراً لارتفاع سعر الجهاز المستخدم في البصمة الإلكترونية [41].

تؤخذ البصمة الإلكترونية وفق الخطوات المتبعة في البصمة التقليدية، ولكن من دون استخدام الحبر التقليدي، بل عن طريق جهاز سكانر خاص مختلف عن ذلك المخصص للصور والوثائق، وهو يخزن بصمة الشخص ويعد هذا الجهاز وحدة عمل متكاملة تشمل أخذ البصمة والتدقيق والمقارنة [42].

بدورنا نرى أن البصمة التقليدية سهلة التزوير نسبياً وتحتاج إلى وقت وجهد في الحفظ والمطابقات، فضلاً عن إنها تعد أقل دقة وابطأ في الإجراءات، أما البصمة الإلكترونية فهيَ تعتمد الوسائل الرقمية وتكون عالية الدقة وسريعة في التحقق وأيضاً تعد صعبة التلاعب عند توافر أنظمة حماية جيدة، فضلاً عن انها تكون سهلة الخزن والتطابق آلياً خلال ثوانٍ، وتعد أكثر انسجاماً مع التطور التقني ومتطلبات الإثبات الحديث.

المبحث الثاني

المسؤولية الجنائية عن التلاعب بأنظمة البصمة الإلكترونية

تتمحور مسؤولية الجنائية عن التلاعب بأنظمة البصمة الالكترونية في بيان أركان الجريمة وكذلك بيان مسؤولية الموظف أو كونه مكلفًا بخدمة عامة وايضاً العقوبات المترتبة عليه في كل من تشريع العراقي والمصري، وسنوضح ذلك في ثلاثة مطالب على نحو الآتي:

المطلب الأول

أركان جريمة التلاعب بأنظمة البصمة الإلكترونية

يتضمن أركان جريمة التلاعب بأنظمة البصمة الإلكترونية ما يأتي:

أولاً: الركن الشرعي (وجود نص يجرّم الفعل)، مع غياب نص قانوني خاص بهذه الجريمة ولكن الجرم يُكيف على وفق إحدى المواد الآتية:

1. التزوير (289–298) من قانون العقوبات العراقي [43].
2. الاحتيال المادة (456) [44].

ثانياً: الركن المادي للجريمة نص المادة 28 من قانون العقوبات العراقي بان الركن المادي للجريمة يتمثل بسلوك إجرامي بارتكاب فعل جرمه القانون أو الامتناع عن فعل أمر به القانون، وبذلك يتحقق بأي فعل يغيّر بيانات البصمة أو يتلاعب بها [45]:

1. السلوك الإجرامي [46]: هو كل نشاط مادي او معنوي يمارسه الإنسان فهو بهذا يستوعب الأفكار والمقاصد والرغبات [47]، والسكنات والمتمثل في تسجيل بصمة موظف آخر بالحضور، تعطيل جهاز البصمة أو إيقافه، تثبيت بصمة مزورة (طباعة سيليكون أو أدوات رقمية)، استخدام برامج لتغيير وقت الحضور والانصراف.
2. النتيجة [48]: تعد النتيجة الإجرامية عنصرا لازماً في تكوين الركن المادي للجريمة ويتمثل في [49]، تسجيل بيانات زائفة في النظام أو الحصول على منفعة وظيفية غير مشروعة أو الإضرار بجهة العمل أو النظام الإلكتروني.
3. العلاقة السببية [50]: الصلة التي تربط ما بين السلوك والنتيجة التي يكتمل بقيامها الركن المادي للجريمة وبذلك يجب أن تكون النتيجة ناتجة عن فعل التلاعب بالبصمة أو النظام [51].

ثالثاً: الركن المعنوي (القصد الجرمي) [52]، يقصد به توجيه الفاعل إرادته إلى ارتكاب الفعل المكون للجريمة هادفاً إلى نتيجة الجريمة التي وقعت أو أية نتيجة جرمية اخرى، والقصد هو الحالة النفسية للجاني والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني [53]، ويتمثل في علم الجاني بعدم مشروعية الفعل واتجاه إرادته إلى تحقيق النتيجة [54]، يتطلب ما يأتي:

1. العلم: أن يكون الجاني عالماً بأن من شأن فعلة هذه أنه يتلاعب [55]، ببصمة ليست له أو يحرف بياناتها.
2. الإرادة: ان تتجه إرادة الجاني إلى ارتكاب الجريمة نحو تحقيق [56]، قصد منفعة (راتب، غياب، تهرب من الدوام ...الخ)، ونرى أن يكون نص قانوني يجرم هذا الأفعال على النحو الآتي: (يعاقب بالسجن مدة لا تزيد على (10) سنوات وبغرامة لا تقل عن (5) ملايين دينار كل من تعمّد التلاعب بأنظمة البصمة الإلكترونية بقصد تغيير بيانات الحضور أو الهوية أو الامتيازات أو حقوق الموظفين).

المطلب الثاني

المسؤولية الجنائية للموظف أو مكلف بخدمة عامة عن التلاعب بأنظمة البصمة الالكترونية

سنوضح في هذا المطلب المسؤولية الجنائية لكل من الموظف أو مكلف بخدمة عامة عن التلاعب بأنظمة البصمة الالكترونية، على

النحو الآتي:

لم تتطرق غالبية القوانين الجزائية إلى تعريف الموظف العام، فبخصوص المشرع العراقي فهو لم ينص صراحة على تعريف الموظف العام في قانون العقوبات الحالي وفي قانون أصول محاكمات الجزائية، ولكن أشار إلى صفة الموظف العام بجانب صفة المكلف بخدمة عامة في مواد متفرقة وفي جرائم متعددة كما ورد في جريمة الرشوة وجرائم الاختلاس وجرائم الاعتداء على الموظفين كركن في الجريمة، وأيضا في جريمة القتل والضرب والسرقة كظرف في الجريمة، وهكذا ربط المشرع العراقي الموظف مع المكلف بخدمة عامة كما أكدت المادة (19/2) من قانون العقوبات العراقي على ذلك [57].

عبرت بعض القوانين الجنائية صراحة عن تعريف الموظف العام بحيث تجاوز إطار التعريف الإداري له ومن قبيل هذه التشريعات قانون العقوبات الأردني، وقانون العقوبات اللبناني، وقانون عقوبات التونسي، والمغربي، والجزائري، وقانون العقوبات الليبي، وقانون العقوبات الإماراتي، وقانون عقوبات سلطنة عمان، وقانون العقوبات السوري [58].

عرف الموظف العام في قانون الخدمة المدنية العراقي بأنه "(هو كل شخص عهدت اليه وظيفة دائمة داخلة في مالك الدولة الخاصة بالموظفين)" [59].

عُرِّف الموظف العام من قانون انضباط موظفي الدولة والقطاع العام العراقي بأنه "(كل شخص عهدت اليه وظيفة داخل مالك الوزارة أو الجهة غير المرتبطة بالوزارة)" [60]، يشير قانون التقاعد العراقي الملغي بأن يسري هذا القانون على جميع الموظفين الدولة والعسكريين ومنتسبي قوى الأمن الداخلي وموظفي الشركات العامة الموجودين في الخدمة بتاريخ نفاذ القانون [61].

عليه وبحسب موقف التشريعات الإدارية في العراق لكي يُعدُّ شخصًا موظفا عاماً يجب أن تتوافر فيه بعض الشروط:

أ- يجب أن يكون الموظف قد تم تعينه بشكل أصولي من الجهة المختصة بالتعيين، وتتوافر فيه الشروط المطلوبة للتعيين.

ب- صدور قرار إداري صريح بالتعيين.

ت- أن يكون قد تم تعيينه موظفا بصفة دائمية في خدمة القطاع العام، ويكون موظفاً إذا كان عمله مؤقتا في خدمة القطاع العام، ويشمل القطاع العام كل دوائر الدولة، وتقوم الدولة بتقديم الخدمات العامة لأفرادها بواسطة الموظفين أو المكلفين بالخدمة العامة ويقومون بإدارة دوائرها وحماية مصالحها ومقابل ذلك يقوم القطاع العام بتحديد حقوقهم وواجباتهم بتنظيمها عِبر قوانين خاصة بهم [62].

أما المكلف بخدمة عامة فقد عرفه قانون العقوبات العراقي المكلف بخدمة عامة بأنه "(كل موظف أو مستخدم أو عامل أنيطت به مهمة عامة في خدمة الحكومة ودوائرها الرسمية وشبه رسمية والمصالح التابعة لها أو الموضوعة تحت رقابتها ويشمل ذلك رئيس الوزراء ونوابه والوزراء واعضاء المجالس النيابية والإدارية والبلدية، كما يشمل المحكمين والخبراء ووكلاء الدائنين والسنديكين والمصفين والحراس القضائيين وأعضاء المجالس الادارة ومديري المؤسسات والشركات والجمعيات والمنظمات ومستخدميها، والمنشأة التي تساهم الحكومة أو إحدى دوائرها الرسمية أو شبه الرسمية في مالها بنصيب ما بأية صفة كانت، وعلى العموم كل من يقوم بخدمة عامة بأجر أو بغير أجر)" [63].

لم يوضح المشرع جريمة التلاعب بأنظمة البصمة الالكترونية ولكن يتبين لنا أن الموظف إذا تلاعب بإحدى أنظمة البصمة الالكترونية فإن عقوبته تكون اشد من الشخص غير الموظف، وعلة التشديد تكمن في أن الصفة المنوطة بالموظف تيسّر له سهولة التلاعب بهذه الأنظمة على خلاف الشخص غير الموظف، ونرى وجوب تشديد العقوبة أسوة بنصوص المواد التي جعلت من صفة الموظف إذا ارتكب الجريمة أشد من غيره، ويكون النص كالآتي: (تُشدّد العقوبة إلى السجن مدة لا تقل عن 10 سنوات إذا ارتُكب الفعل من موظف أو مكلف بخدمة عامة استغل وظيفته أو صلاحياته للوصول إلى النظام أو تعطيله أو إدخال بيانات مزوّرة).

لكن بالعودة الى مشروع قانون مكافحة الجرائم المعلوماتية العراقي رقم 2019 اوضح المشروع وفي نص خاص إلى تشديد العقوبة في حال ارتكاب الجريمة من موظف أو مكلف بخدمة عامة [64].

المطلب الثالث

التكييف القانوني للتلاعب بأنظمة البصمة الإلكترونية والعقوبة المترتبة عليها

سنستعرض في هذا المطلب عقوبة الجريمة مع إمكانية بيان تطبيق النصوص القانونية الموضحة لها في كل من التشريعين العراقي والمصري، على النحو الآتي:

أولاً: القانون العراقي.

لا يوجد نص خاص في قانون العقوبات العراقي يجرّم "التلاعب بالبصمة الإلكترونية" مباشرة، لكن يُعالج الفعل عبر قواعد عدة:

1. التزوير، والاحتيال، أو خيانة الأمانة، ولا يوجد نص محدد باسم "التلاعب بالبصمة الإلكترونية"، لذلك يتم التكييف على وفق الجرائم المماثلة في قانون العقوبات وقانون جرائم المعلوماتية، إذا قام شخص بتزوير البصمة، مثل استنساخ

بصمة موظف لتسجيل حضوره أو التلاعب بساعات الدوام، فإن الفعل يُعدّ تزويرًا، ويعاقب التزوير إذا كان المحرر رسميًّا السجن لمدة لا تزيد على خمس عشرة سنة اما إذا كان المحرر غير رسمي السجن لمدة لا تزيد عن سبع سنوات او الحبس [65].

2. استخدام بصمة شخص آخر: الدخول إلى النظام الإلكتروني باستخدام بصمة غيره يُصنّف كـ احتيال وتكون العقوبة الحبس [66].
3. تعطيل أو تخريب جهاز البصمة تلف أو تعطيل أجهزة البصمة الحكومية: يُعد إتلاف مال الدولة وفق المادة (340) يعاقب بالسجن مدة لا تزيد على سبع سنوات أو بالحبس [67]، وإذا كان الجهاز ملكاً لغيره فتطبق المادة (477) يعاقب بالحبس مدة لا تزيد على سنتين وبغرامة لا تزيد على مائتي دينار أو بإحدى هاتين العقوبتين وكذلك يعاقب بالحبس أما إذا ترتب على الجريمة موت إنسان فتكون العقوبة السجن [68]، وكذلك تصنيع وبيع واستيراد أدوات التي تساعد على التلاعب بأنظمة البصمة الالكترونية يجب المعاقبة عليها ويكون النص كالآتي: (يُعاقب بالحبس والغرامة كل من يصنع أو يبيع أو يشتري أو يستورد أي أدوات أو برمجيات تهدف إلى التحايل على أنظمة البصمة الإلكترونية، أو توليد بصمات مزيفة، أو تجاوز نظام التحقق البيومتري).

يتمثل الجزاءات الإدارية في قانون انضباط موظفي الدولة والقطاع العام رقم 14 لسنة 1991 نص المادة 8 أن العقوبات التي يجوز فرضها على الموظف "(لفت النظر، الإنذار، قطع الراتب، التوبيخ، إنقاص الراتب، تنزّل الدرجة، الفصل، العزل)" [69].

ثانياً: القانون المصري.

هناك تشريع مباشر للبيانات البيو مترية والجرائم الإلكترونية، لذا يجب أن تكون العقوبات واضحة وصارمة إذ وُضعت وضع عقوبات إدارية فضلاً عن عقوبات جنائية كما يأتي:

أ) الجزاءات الإدارية مادة (٣٠): مع عدم الإخلال بأحكام المسؤولية المدنية والجنائية، يقوم الرئيس التنفيذي للمركز، في حال ارتكاب أي مخالفة لأحكام هذا القانون بإنذار المخالف بالتوقف عن المخالفة وإزالة أسبابها أو آثارها خلال مدة زمنية يحددها، فإذا انقضت المدة المشار إليها دون تنفيذ مضمون ذلك الإنذار، كان لمجلس إدارة المركز أن يصدر قرارًا مسببًا بما يأتي:

1. الإنذار بإيقاف الترخيص أو التصريح أو الاعتماد جزئيًا أو كليًا لمدة محددة.
2. إيقاف الترخيص أو التصريح أو الاعتماد جزئيًا أو كليًا.
3. سحب الترخيص أو التصريح أو الاعتماد أو إلغاؤه جزئيًا أو كليًا.
4. نشر بيان بالمخالفات التي ثبت وقوعها في وسيلة إعلام أو أكثر واسعة الانتشار على نفقة المخالف.
5. إخضاع المتحكم أو المعالج للإشراف الفني للمركز لتأمين حماية البيانات الشخصية على نفقتهما بحسب الأحوال [70].

ب) العقوبات الجنائية [71]، نص المادة (٣٥): مع عدم الإخلال بأي عقوبة أشد منصوص عليها في أي قانون آخر، ومع عدم الإخلال بحق المتضرر في التعويض، يعاقب على الجرائم المنصوص عليها في المواد الآتية بالعقوبات المقررة لها [72].

نص المادة (٣٦): يعاقب بغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه كل حائز أو متحكم أو معالج جمع أو عالج أو أفشي أو أتاح أو تداول بيانات شخصية معالجة إلكترونيًا بأي وسيلة من الوسائل في غير الأحوال المصرح بها قانونًا أو بدون موافقة الشخص المعني بالبيانات.

تكون العقوبة الحبس مدة لا تقل عن ستة شهور وبغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه، أو بإحدى هاتين العقوبتين، إذا ارتكب ذلك مقابل الحصول على منفعة مادية أو أدبية، أو بقصد تعريض الشخص المعني بالبيانات للخطر أو الضرر [73].

الخاتمة

بعد الانتهاء من البحث لابد لنا أن نبين أهم ما توصلنا إليه من الاستنتاجات ومقترحات، وسنعرضها فيما يأتي:

أولاً: الاستنتاجات

1. غياب تعريف صريح في قانون العقوبات العراقي للبصمة إذ لا يحتوي على تعريف مباشر لـ "البصمة الإلكترونية".
2. البصمة الإلكترونية وسيلة لـإثبات الحضور والانصراف باستخدام الخصائص البيو مترية للفرد، كالخطوط الفريدة لبصمة الإصبع، وتحويلها إلى بيانات رقمية تُخزن وتُستخدم للتحقق من هوية الشخص ويتمثل أنواع المعرفات البيو مترية كالتعرف على الوجه، الصوت، بصمات الأصابع، مسح الشبكية والقزحية ...الخ.
3. وضح قانون حماية البيانات الشخصية المصري بقوله "البيانات الشخصية أي بيانات متعلقة بشخص طبيعي محدد،

أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى كالاسم، أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية".

4. لا يوجد نص خاص في قانون العقوبات العراقي يجرّم "التلاعب بالبصمة الإلكترونية" مباشرة، لكن يُعالج الفعل عبر قواعد التزوير، الاحتيال، أو خيانة الأمانة الوظيفية، أما المشرع المصري يعاقب على الجزاءات الإدارية مادة (٣٠) فضلاً عن عقوبات جنائية نص المادة (35-36).

ثانياً: المقترحات

1. نهيب بالمشرع العراقي إدراج نص قانوني مستقل لتعريف البصمة الإلكترونية على النحو الآتي (كل بيانات بيو مترية رقمية تُسجَّل أو تُعالَج بواسطة أنظمة إلكترونية بهدف التحقق من هوية الشخص، وتشمل بصمة الإصبع، وبصمة الوجه، وبصمة العين، أو أي نمط بيومتري آخر).
2. نهيب بالمشرع العراقي تجريم التلاعب بالبصمة الإلكترونية كجريمة مستقلة على النحو الآتي (يعاقب بالسجن مدة لا تزيد على (10) سنوات وبغرامة لا تقل عن (5) ملايين دينار كل من تعمّد التلاعب بأنظمة البصمة الإلكترونية بقصد تغيير بيانات الحضور أو الهوية أو الامتيازات أو حقوق الموظفين).
3. نهيب بالمشرع العراقي تشديد العقوبة إذا كان الجاني موظفاً أو مكلفًا بخدمة عامة (تُشدّد العقوبة إلى السجن مدة لا تقل عن 10 سنوات إذا ارتُكب الفعل موظف أو مكلف بخدمة عامة استغل وظيفته أو صلاحياته للوصول إلى النظام أو تعطيله أو إدخال بيانات مزوّرة).
4. نهيب بالمشرع العراقي تجريم صناعة أو تداول أدوات التلاعب (يُعاقب بالحبس والغرامة كل من يصنع أو يبيع أو يشتري أو يستورد أي أدوات أو برمجيات تهدف إلى التحايل على أنظمة البصمة الإلكترونية، أو توليد بصمات مزيفة، أو تجاوز نظام التحقق البيومتري).

الهوامش

(1) عادل يوسف الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة جامعة الكوفة كلية القانون، ع7، 2008، ص112.

(2) إبراهيم مصطفى، المعجم الوسيط، دار الدعوة، إسطنبول، تركيا، 1989م، باب الباء، ص60

(3) المنجد في اللغة العربية المعاصرة، دار المشرق، بيروت، لبنان، 2000م، ص 97.

(4) المصدر نفسه، ص94.

(5) محمد بن مكرم ابي الفضل جمال الدين، لسان العرب، مج1، ط1، بيروت، لبنان، ص29.

(6) فؤاد عبد المنعم احمد، البصمة الوراثية ودورها في الاثبات الجنائي بين الشريعة والقانون، المكتبة المصرية، الاسكندرية، مصر، ص13.

(7) ذكر في مشروع قانون مكافحة الجرائم المعلوماتية العراقي على بيان الجرائم الالكترونية.

(8) راشد بن علي بن حمد، علم البصمات الجنائي، كلية العلوم الأدلة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2008م، ص24.

(9) المادة 1\1 من مشروع قانون مكافحة الجرائم المعلوماتية العراقي لسنة ٢٠١٩.

(10) وجيه العاني وعلي الموسوي، اتجاهات العاملين بالجامعات نحو تطبيق البصمة الالكترونية وعلاقتها بالولاء التنظيمي بسلطنة عمان، عمان، الأردن، 2019م، ص10.

(11) المصدر نفسه، ص11.

(12) قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020.

(13) نص المادة (1) من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020.

(14) نبيلة رزاقي، الحماية الجنائية للخصوصية الرقمية للمعطيات ذات الطابع الشخصي دراسة مقارنة، مجلة الدراسات القانونية المقارنة، مج 7، ع1، 2020م، ص 1999.

(15) Biometric Technology and Ethics: Beyond Security Applications ،Published: 08 March 2019 ، Volume 167, pages 433–450, (2020).

(16) كيري هولواي وريم المصري وافنان أبو يحيى، الهوية الرقمية والبيانات البيومترية والادماج في الاستجابات الإنسانية لازمات اللاجئين، ورقة عمل فريق السياسات الإنسانية (HPG)، 2021م، منشورة على الرابط https://media.odi.org/documents/ARABIC_Digital_IP_Biometrics_case_study_WEB.pdf ، ص6.

(17) Nathalie Mallet –poujol، Protection de la vie privée et des données personnelles، op. cit ، n° 79، 80 et 81.

(18) د. علي دريول الجبوري، الحوكمة الرقمية التسجيل البايومتري وتحديات الخصوصية، المجلة السياسية الدولية، ع63، 2025م، ص 210.

(19) د. خالد محمد علي، الحماية القانونية للبيانات الشخصية في أطار القانون المدني دراسة مقارنة، مجلة كلية القانون للعلوم القانونية والسياسية، مج 12، ع47، 2023م، ص230.

(20) ينظر د. أبو هشيمة كامل الجبالي، حماية البيانات الشخصية في البيئة الرقمية، بحث مقدم الى مؤتمر العصر الرقمي واشكالياته القانونية، كلية الحقوق، جامعة أسيوط، 2016م، ص 4.

(21) د. علي دريول الجبوري، الحوكمة الرقمية التسجيل البايومتري وتحديات الخصوصية، المجلة السياسية الدولية، ع63، 2025م، ص 213.

(22) cumplimiento del RGPD ،noviembre 25، 2024 https://veridas.com/es/que-son-los-datos-biometricos/.

(23) مداح فاتح، علاقة تطبيق نظام البصمة الالكترونية بأداء الموظفين، دراسة ميدانية بكلية العلوم الإنسانية والاجتماعية بجامعة محمد بوضياف –المسيلة-، رسالة ماجستير، 2020م، ص13-14.

(24) المصدر نفسه، ص 14.

(25) محمود محافظي، البصمات كدليل علمي وحجيتها في الاثبات الجنائي، رسالة ماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، 2012م، ص20.

(26) منصور عمر المعايطة، الطب الشرعي في خدمة الأمن والقضاء، مكتبة الملك فهد، الرياض، السعودية، 2007م، ص79.

(27) مداح فاتح، المصدر السابق، ص11.

(28) سورة يوسف الآية (94).

(29) مداح فاتح، المصدر السابق، ص12.

(30) حسين إبراهيم السماحي، استخدام الأساليب العلمية المقدمة لمساندة البحث الجنائي، الاسكندرية، مصر، 1989م، ص13.

(31) آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط2، الجزائر، 2007م، ص100.

(32) UNODC, Comprehensive Study on Cybercrime, 2013، https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

(33) سمية الحمداني، الاثبات الجنائي في العصر الرقمي نحو نظام ذكي للتحقق من مصداقية الادلة الالكترونية، 2025م، بحث منشور على موقع مجلس القضاء الأعلى https://sjc.iq/view.77460/.

(34) شمس نظير وخضر فوزي، علم البصمات دراسة تطبيقية شاملة، دار مكتبة الحياة، بيروت، لبنان، 1984م، ص17.

(35) نقلاً: عن نوميد سعيد خضر، دور الصفة الوظيفية كركن في الجريمة (دراسة تحليلية مقارنة)، مجلة قه لاى زانست العلمية، مج5، ع4، العراق، 2020م، ص10.

(36) عبد الفتاح ريما، البصمة الالكترونية لضبط دوام الموظفين جامعة الامارات العربية المتحدة، دبي الامارات، 2011م، ص8.

(37) مقال استخدام المعلومات البيومترية للتحقق من الهوية منشور على الموقع الالكتروني https://www.fraud.com/post/biometric-information .

(38) نقلاً: عن نوميد سعيد خضر، المصدر السابق، ص2.

(39) مقال الفرق بين البصمة التقليدية والبصمة الالكترونية منشور على الموقع الالكتروني https://anakidalverh.wordpress.com/2013/12/05/ .

(40) مقال الفرق بين البصمة التقليدية والبصمة الالكترونية، المصدر السابق.

(41) مقال الفرق بين البصمة التقليدية والبصمة الالكترونية، المصدر السابق.

(42) مقال الفرق بين البصمة التقليدية والبصمة الالكترونية، المصدر السابق.

(43) المواد (289–298) من قانون العقوبات العراقي رقم 111 لسنة 1969.

(44) المادة (456) من قانون العقوبات العراقي رقم 111 لسنة 1969

(45) ايمان فاضل السامرائي، نظم المعلومات الإدارية، دار صفاء للنشر والتوزيع، الأردن، 2010م، ص141.

(46) نص المادة 28 من قانون العقوبات العراقي "سلوك إجرامي بارتكاب فعل جرمه القانون أو الامتناع عن فعل أمر به القانون".

(47) د. جلال ثروت، قانون العقوبات –القسم العام – منشورات الحلبي الحقوقية، لبنان، 2005 ص1.

(48) المادة 29\1 من قانون العقوبات العراقي "لا يسال شخص عن جريمة لم تكن نتيجة لسلوكه الاجرامي لكنه يسال عن الجريمة ولو كان قد ساهم مع سلوكه الاجرامي في احداثها سبب اخر سابق او معاصر او لاحق ولو كان يجهله".

(49) د. سمير الشناوي، الشروع في الجريمة، دراسة مقارنة، دار النهضة العربية، القاهرة، 1971، ص78.

(50) نص المادة 29\2 من قانون العقوبات العراقي "اما إذا كان ذلك السبب وحده كافيا لأحداث نتيجة جرمية فلا يسال الفاعل في هذه الحالة الا عن الفعل الذي ارتكبه".

(51) د. عمر فاروق الحسيني، تعذيب المتهم لحمله على الاعتراف، الجريمة والمسؤولية، المطبعة العربية الحديثة، 1986م، ص177.

(52) نص المادة 33 من قانون العقوبات العراقي "القصد الجرمي هو توجيه الفاعل ارادته الى ارتكاب الفعل المكون للجريمة هادفا الى نتيجة الجريمة التي وقعت او اية نتيجة جرمية أخرى".

(53) محمد امين الرومي، جرائم الكمبيوتر والانترنيت، دار المطبوعات الجامعية، لبنان، 2008م، ص98.

(54) محمود نجيب حسني، شرح قانون العقوبات، القسم العام، ط2، دار النهضة العربية القاهرة، م1984، ص201.

(55) د. عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة الكترونيا دراسة مقارنة، دار النهضة العربية، القاهرة، 2010م، ص716.

(56) د. احمد شوقي أبو خطوة، شرح الاحكام العامة لقانون العقوبات، دار النهضة العربية، القاهرة، 2003م، ص87-89.

(57) المادة 19\2 من قانون العقوبات العراقي.

(58) ينظر المادة 169من قانون العقوبات الاردني، والمادة 383 من قانون العقوبات اللبناني والمادة 82 من قانون العقوبات التونسي والمادة 224 من قانون العقوبات المغربي والمادة 149 من قانون العقوبات الجزائري، والمادة 16/4 من قانون العقوبات الليبي، والمادة /2ب من قانون العقوبات الإماراتي، والمادة 154 من قانون عقوبات سلطنة عمان والمادة 340 من قانون العقوبات السوري.

(59) المادة (2) من قانون الخدمة المدنية رقم 24 لسنة 1960المعدل.

(60) المادة (1) من قانون انضباط موظفي الدولة والقطاع العام رقم 14لسنة1991المعدل.

(61) المادة (29) من قانون التقاعد العراقي رقم 27 لسنة 2006 الملغي.

(62) نقلاً: عن ئوميد سعيد خضر، المصدر السابق، ص508.

(63) المادة 19\2 من قانون العقوبات العراقي.

(64) المادة 4\5 الفصل الثاني (الجرائم والعقوبات) من مشروع قانون مكافحة الجرائم المعلوماتية العراقي لسنة ٢٠١٩.

(65) المواد 289–290 من قانون العقوبات العراقي رقم 111 لسنة 1969.

(66) المادة 456 من قانون العقوبات العراقي.

(67) نص المادة 430 من قانون العقوبات العراقي " ...كل موظف او مكلف بخدمة عامة أحدث عمدا ضررا بأموال او مصالح الجهة التي يعمل فيها او يتصل بها بحكم وظيفته او بأموال الاشخاص المعهود بها اليه".

(68) نص المادة 477 من قانون العقوبات العراقي رقم 111 لسنة 1969.

(69) نص المادة 8 من قانون انضباط موظفي الدولة والقطاع العام رقم 14 لسنة 1991.

(70) قانون حماية البيانات الشخصية لسنة 2020 الفصل العاشر التراخيص والتصاريح والاعتمادات نص المادة 30.

(71) قانون حماية البيانات الشخصية لسنة 2020 الفصل الرابع عشر الجرائم والعقوبات نصوص المواد 35 إلى 48.

(72) قانون حماية البيانات الشخصية لسنة 2020 الفصل الرابع عشر الجرائم والعقوبات نص المادة 35.

(73) قانون حماية البيانات الشخصية لسنة 2020 الفصل الرابع عشر الجرائم والعقوبات نص المادة 36.

المصادر

- **القرآن الكريم**

أولاً- معاجم اللغة

- إبراهيم مصطفى، المعجم الوسيط، دار الدعوة، إسطنبول، تركيا، 1989م، باب الباء.
- محمد بن مكرم ابي الفضل جمال الدين، لسان العرب، مج1، ط1، بيروت، لبنان.
- المنجد في اللغة العربية المعاصرة، دار المشرق، بيروت، لبنان، 2000م.

ثانياً- الكتب القانونية

- آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط2، الجزائر، 2007م.

- ايمان فاضل السامرائي، نظم المعلومات الإدارية، دار صفاء للنشر والتوزيع، الأردن، 2010م.
- حسين إبراهيم السماحي، استخدام الأساليب العلمية المقدمة لمساندة البحث الجنائي، الاسكندرية، مصر، 1989م.
- د. احمد شوقي أبو خطوة، شرح الاحكام العامة لقانون العقوبات، دار النهضة العربية، القاهرة، 2003م.
- د. جلال ثروت، قانون العقوبات –القسم العام – منشورات الحلبي الحقوقية، لبنان، 2005م.
- د. سمير الشناوي، الشروع في الجريمة، دراسة مقارنة، دار النهضة العربية، القاهرة، 1971م.
- د. عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة الكترونيا دراسة مقارنة، دار النهضة العربية، القاهرة، 2010م.
- د. عمر فاروق الحسيني، تعذيب المتهم لحمله على الاعتراف، الجريمة والمسؤولية، المطبعة العربية الحديثة، 1986م.
- راشد بن علي بن حمد، علم البصمات الجنائي، كلية العلوم الأدلة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2008م.
- شمس نظير وخضر فوزي، علم البصمات دراسة تطبيقية شاملة، دار مكتبة الحياة، بيروت، لبنان، 1984م.
- عبد الفتاح ريما، البصمة الالكترونية لضبط دوام الموظفين جامعة الامارات العربية المتحدة، دبي الامارات، 2011م.
- فؤاد عبد المنعم احمد، البصمة الوراثية ودورها في الاثبات الجنائي بين الشريعة والقانون، المكتبة المصرية، الاسكندرية، مصر.
- محمد امين الرومي، جرائم الكمبيوتر والانترنيت، دار المطبوعات الجامعية، لبنان، 2008م.
- محمود نجيب حسني، شرح قانون العقوبات، القسم العام، ط2، دار النهضة العربية القاهرة، م1984.
- منصور عمر المعايطة، الطب الشرعي في خدمة الأمن والقضاء، مكتبة الملك فهد، الرياض، السعودية، 2007م.
- وجيه العاني وعلي الموسوي، اتجاهات العاملين بالجامعات نحو تطبيق البصمة الالكترونية وعلاقتها بالولاء التنظيمي بسلطنة عمان، عمان، الأردن، 2019م.

ثالثاً- الرسائل الجامعية

- محمود محافظي، البصمات كدليل علمي وحجيتها في الاثبات الجنائي، رسالة ماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، 2012م.
- مداح فاتح، علاقة تطبيق نظام البصمة الالكترونية بأداء الموظفين، دراسة ميدانية بكلية العلوم الإنسانية والاجتماعية بجامعة محمد بوضياف –المسيلة-، رسالة ماجستير، 2020م.

رابعاً- المجلات والأبحاث القانونية

- د. أبو هشيمة كامل الجبالي، حماية البيانات الشخصية في البيئة الرقمية، بحث مقدم الى مؤتمر العصر الرقمي واشكالياته القانونية، كلية الحقوق، جامعة أسيوط، 2016م.
- د. خالد محمد علي، الحماية القانونية للبيانات الشخصية في أطار القانون المدني دراسة مقارنة، مجلة كلية القانون للعلوم القانونية والسياسية، مج 12، ع47، 2023م.
- د. علي دريول الجبوري، الحوكمة الرقمية التسجيل البايومتري وتحديات الخصوصية، المجلة السياسية الدولية، ع63، 2025م.
- عادل يوسف الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة جامعة الكوفة كلية القانون، ع7، 2008م.
- نبيلة رزاقي، الحماية الجنائية للخصوصية الرقمية للمعطيات ذات الطابع الشخصي دراسة مقارنة، مجلة الدراسات القانونية المقارنة، مج 7، ع1، 2020م.
- ئوميد سعيد خضر، دور الصفة الوظيفية كركن في الجريمة (دراسة تحليلية مقارنة)، مجلة قه لاى زانست العلمية، مج5، ع4، العراق، 2020م.

خامساً- القوانين العراقية والعربية

أ. القوانين العراقية

- قانون التقاعد العراقي رقم 27 لسنة 2006 الملغي.
- قانون الخدمة المدنية رقم 24 لسنة 1960المعدل.
- قانون العقوبات العراقي رقم 111 لسنة 1969.
- قانون انضباط موظفي الدولة والقطاع العام رقم 14لسنة1991المعدل.
- مشروع قانون مكافحة الجرائم المعلوماتية العراقي لسنة ٢٠١٩.

ب. القوانين العربية

- قانون العقوبات الأردني.
- قانون العقوبات الإماراتي.
- قانون العقوبات التونسي.
- قانون العقوبات الجزائري.
- قانون العقوبات السوري.
- قانون العقوبات اللبناني.
- قانون العقوبات الليبي.
- قانون العقوبات المغربي.
- قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020.
- قانون عقوبات سلطنة عمان.

سادساً- المواقع الالكترونية

- cumplimiento del RGPD ،noviembre 25، 2024 https://veridas.com/es/que-son-los-datos-biometricos\
- José Miguel Sánchez Digital Identity consultant Datos biométricos: qué son، definición، ejemplos y cumplimient del RGPD ،noviembre 25، 2024 https://veridas.com/es/que-son-los-datos-biometricos/.
- UNODC, Comprehensive Study on Cybercrime, 2013، https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
- سمية الحمداني، الاثبات الجنائي في العصر الرقمي نحو نظام ذكي للتحقق من مصداقية الادلة الالكترونية، 2025م، بحث منشور على موقع مجلس القضاء الأعلى https://sjc.iq/view.77460/.
- كيري هولواي وريم المصري وافنان أبو يحيى، الهوية الرقمية والبيانات البيومترية والادماج في الاستجابات الإنسانية لازمات اللاجئين، ورقة عمل فريق السياسات الإنسانية (HPG)، 2021م، منشورة على الرابط https://media.odi.org/documents/ARABIC_Digital_IP_Biometrics_case_study_WEB.pdf .
- مقال استخدام المعلومات البيومترية للتحقق من الهوية منشور على الموقع الالكتروني https://www.fraud.com/post/biometric-information.