Vol. 3, No. 1, pp. 333-352 | 2025
CFORSJ Procedia

الحماية الإدارية للبيانات الشخصية بين التشريعات الوطنية والمبادئ الدولية للحوكمة: دراسة مقارنة

ADMINISTRATIVE PROTECTION OF PERSONAL DATA BETWEEN NATIONAL LEGISLATION AND INTERNATIONAL GOVERNANCE PRINCIPLES: A COMPARATIVE STUDY

[i,*]Mohamed Abdalla Alhammadi & [i]Wan Abdul Fattah Wan Ismail

[i]Faculty of Syariah and Law, USIM, Universiti Sains Islam Malaysia, Bandar Baru Nilai, Malaysia

*(Corresponding author) e-mail: Bojasem6445@hotmail.com

ABSTRACT

This study examines the administrative protection of personal data within a comparative framework between national legislation in the United Arab Emirates and the Arab Republic of Egypt and international governance principles. This study examines the growing strategic importance of data as a fundamental pillar of the digital economy and a sensitive area of human rights. The study adopted a comparative analytical approach supported by critical institutional analysis, where Federal Decree-Law No. (45) of 2021 in the UAE and Law No. (151) of 2020 in Egypt were analyzed and compared with the European General Data Protection Regulation (GDPR), which constitutes the most advanced model globally. The results showed that Emirati legislation is characterized by comprehensiveness and the recognition of direct individual rights such as the right to rectification, erasure, and objection, while Egyptian legislation focused on an institutional approach by establishing a Personal Data Protection Center with broad licensing and oversight powers. Despite this divergence in legislative philosophy, the study reveals that both models face similar challenges, namely the weak independence of administrative bodies, insufficient technical capabilities, and limited administrative penalties compared to the stringency of European sanctions, which impose strict and deterrent obligations on violating institutions. It also reveals that governance principles such as transparency, accountability, and fairness are partially reflected in legal texts but have not yet been transformed into integrated institutional practices capable of ensuring compliance. The study concludes that administrative protection in the UAE and Egypt is still in its infancy, requiring legislative and institutional reforms, most notably strengthening the independence of oversight bodies, enhancing the level of penalties to be deterrent, developing human and technical capabilities, and activating regional and international cooperation to address cross-border challenges. The study thus provides a scholarly contribution that fills a gap in the Arab literature and links national protection with international governance standards.

Keywords: *Administrative protection of personal data, national legislation, governance principles, digital privacy, comparative legislation*

ملخص البحث

تتناول هذه الدراسة الحماية الإدارية للبيانات الشخصية في إطار مقارن بين التشريعات الوطنية في كل من دولة الإمارات العربية المتحدة وجمهورية مصر العربية والمبادئ الدولية للحوكمة، وذلك في ظل تزايد الأهمية الاستراتيجية للبيانات باعتبارها ركيزة أساسية للاقتصاد الرقمي ومجالًا حساسًا لحقوق الإنسان. اعتمد البحث المنهج المقارن التحليلي مدعومًا بالتحليل المؤسسي النقدي، حيث تم تحليل المرسوم بقانون اتحادي رقم (45) لسنة 2021 في الإمارات والقانون رقم (151) لسنة 2020 في مصر، ومقارنتهما باللائحة الأوروبية لحماية البيانات (GDPR) التي تشكل النموذج الأكثر تقدمًا عالميًا. أظهرت النتائج أن التشريع الإماراتي اتسم بالشمولية وإقرار حقوق فردية مباشرة مثل الحق في التصحيح والمحو والاعتراض، في حين ركز التشريع المصري على المقاربة المؤسسية عبر إنشاء مركز حماية البيانات الشخصية بسلطات واسعة في الترخيص والرقابة. ورغم هذا التباين في الفلسفة التشريعية، كشفت الدراسة أن كلا النموذجين يواجه تحديات متشابهة تتمثل في ضعف استقلالية الأجهزة الإدارية، وقصور الكفاءات الفنية، ومحدودية الجزاءات الإدارية مقارنة بصرامة العقوبات الأوروبية التي تفرض التزامات صارمة وردعية على المؤسسات المخالفة. كما تبين أن مبادئ الحوكمة مثل الشفافية والمساءلة والعدالة انعكست جزئيًا في النصوص القانونية لكنها لم تتحول بعد إلى ممارسات مؤسسية متكاملة قادرة على ضمان الامتثال. وتخلص الدراسة إلى أن الحماية الإدارية في الإمارات ومصر ما تزال في مرحلة تأسيسية تتطلب إصلاحات تشريعية ومؤسسية، أبرزها تعزيز استقلالية الأجهزة الرقابية، ورفع مستوى الجزاءات لتكون رادعة، وتطوير القدرات البشرية والتقنية، إلى جانب تفعيل التعاون الإقليمي والدولي لمواجهة التحديات العابرة للحدود، وبذلك تقدم الدراسة إسهامًا علميًا يسد فجوة في الأدبيات العربية ويربط بين الحماية الوطنية والمعايير الدولية للحوكمة.

الكلمات المفتاحية: الحماية الإدارية للبيانات الشخصية، التشريعات الوطنية، مبادئ الحوكمة، الخصوصية الرقمية، التشريع المقارن

المقدمة

شهد العالم خلال العقود الأخيرة طفرة غير مسبوقة في مجال تكنولوجيا المعلومات والاتصالات، أدت إلى تحويل البيانات الشخصية من مجرد عناصر ثانوية تُستخدم في إدارة شؤون الأفراد اليومية إلى مورد استراتيجي بالغ الأهمية يماثل في قيمته الاقتصادية والسياسية الموارد الطبيعية التقليدية. فقد باتت البيانات الشخصية تشكل الوقود الرئيس للاقتصاد الرقمي، إذ تُسهم في بناء قواعد البيانات الضخمة التي تعتمد عليها الشركات العالمية في رسم استراتيجياتها، كما تؤثر مباشرة في صياغة السياسات العامة، وتعيد تشكيل أنماط التفاعل الاجتماعي والسياسي على حد سواء (Al-Bustani، 2025). ومع ذلك، فإن هذه الأهمية المتزايدة جعلت البيانات عرضة لانتهاكات متعددة، ليس

فقط من جانب الأفراد أو الشركات الخاصة الباحثة عن تحقيق مكاسب اقتصادية، بل كذلك من قِبل بعض أجهزة الدولة التي قد تبرر تدخلها بمقتضيات الأمن القومي أو المصلحة العامة، وهو ما أدى إلى زيادة الحاجة إلى تشريعات وطنية قادرة على إرساء قواعد قانونية واضحة تضمن حماية فعالة لهذه البيانات ضمن إطار من التوازن بين الحقوق الفردية ومتطلبات المصلحة العامة.

في هذا السياق، برزت تشريعات وطنية عربية حديثة في كل من الإمارات ومصر باعتبارها خطوات جادة نحو مواكبة المعايير الدولية، حيث أصدر المشرع الإماراتي المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية، وهو تشريع تميز بالشمولية وتبنى فلسفة قريبة من اللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR)، بينما اعتمد المشرع المصري القانون رقم (151) لسنة 2020 الذي ركز بدرجة أكبر على إنشاء "مركز حماية البيانات الشخصية" كجهاز إداري له سلطات واسعة في منح التراخيص ومراقبة الامتثال (Mahmoud، 2022). ومن هنا يتضح أن التجربتين تعكسان وعيًا متناميًا بأهمية حماية الخصوصية كحق أساسي، ولكنهما تختلفان في فلسفة الحماية: الإمارات تميل إلى إعطاء الأفراد أدوات قانونية مباشرة، بينما تركز مصر على المقاربة المؤسسية والتنظيمية.

وتكمن أهمية حماية البيانات الشخصية في كونها تمثل صلة مباشرة بين الحق في الخصوصية ومبادئ الحوكمة الرشيدة. إذ إن البيانات الشخصية — بما تحمله من معلومات حساسة تتعلق بالهوية، والوضع الصحي، والنشاط الاقتصادي — تُعد من أكثر الحقوق عرضة للانتهاك في العصر الرقمي، وهو ما يجعل صيانتها جزءًا لا يتجزأ من احترام الكرامة الإنسانية (Osman، 2025). وتؤكد الدراسات الحديثة أن الأهمية العملية لحماية البيانات لا تنحصر في مواجهة الجرائم المعلوماتية أو الاعتداءات الرقمية، وإنما تشمل كذلك تمكين الأفراد من ممارسة سيادتهم على بياناتهم والتحكم في مصيرها، من خلال الاطلاع عليها، أو طلب تصحيحها، أو المطالبة بمحوها عند الاقتضاء (Abu Khumra، 2021). وهذا التوجه ينسجم بشكل وثيق مع الاتجاهات العالمية التي أرستها اللائحة العامة لحماية البيانات (GDPR)،

والتي باتت تمثل معيارًا دوليًا يحتذى به في مجال تعزيز حقوق الأفراد في مواجهة السلطات والمؤسسات الخاصة على حد سواء.

ومع ذلك، فإن التحديات المرتبطة بالتطبيق العملي تظل عقبة أساسية أمام تحقيق الحماية الفعلية. فالقوانين يمكن أن تؤسس لمبادئ عامة، غير أن فاعليتها تتوقف على وجود مؤسسات إدارية قادرة على مراقبة الامتثال، وتوقيع الجزاءات عند الضرورة، وتقديم الدعم الفني للأفراد والمؤسسات. ففي الإمارات، أنشئ "مكتب حماية البيانات" كجهاز إشرافي ورقابي يتولى هذه المهام، بينما أُنشئ في مصر "مركز حماية البيانات الشخصية" للقيام بالدور نفسه (Al-Hinai، 2025؛ Al-Bustani، 2025). غير أن هذه الأجهزة تواجه تحديات عملية متشعبة، من أبرزها محدودية الموارد البشرية المؤهلة، وندرة الخبرات التقنية المتخصصة، إضافة إلى تداخل الصلاحيات بين السلطات

الإدارية المختلفة. كما أن هذه المؤسسات تجد نفسها أحيانًا أمام معضلة صعبة تتمثل في الموازنة بين متطلبات حماية البيانات واعتبارات الأمن القومي أو المصالح الاقتصادية الكبرى، الأمر الذي قد يؤدي إلى تقليص مساحة الحماية الفعلية على أرض الواقع (Al-Qatatsha، 2022).

وتزداد هذه الإشكالية وضوحًا عند تحليل نظام الجزاءات الإدارية. فالجزاءات مثل الإنذار، أو سحب الترخيص، أو نشر بيانات المخالفين على العلن قد تشكل أدوات ردع فعالة، لكنها في الوقت ذاته تثير جدلًا حول مدى اتساقها مع الضمانات الدستورية لحرية التعبير وحرية النشاط الاقتصادي. وهذا يبرز الحاجة إلى صياغة منظومة جزائية أكثر توازنًا تضمن الردع دون المساس بالحقوق الدستورية (Al-Barwani، 2022).

وعلى المستوى الدولي، فإن المبادئ العامة للحوكمة تضع إطارًا مرجعيًا يعزز من ضرورة أن تكون حماية البيانات جزءًا لا يتجزأ من منظومة الحوكمة الرشيدة. فالمساءلة تقتضي إخضاع جميع الجهات التي تجمع أو تعالج البيانات لرقابة صارمة، والشفافية تفترض وضوح إجراءات جمع البيانات وأغراض استخدامها أمام الأفراد، في حين أن العدالة والمساواة تعنيان ضمان تطبيق القواعد القانونية بشكل متساوٍ ودون تمييز (Ibrahim، 2025). وقد عززت أحكام المحكمة الأوروبية لحقوق الإنسان هذا الاتجاه من خلال ربط حماية البيانات بالحق في احترام الحياة الخاصة المنصوص عليه في المادة (8) من الاتفاقية الأوروبية لحقوق الإنسان (Hussein، 2020). كما أن اللائحة الأوروبية (GDPR) جسدت عمليًا هذه المبادئ عندما فرضت التزامات دقيقة على المؤسسات، وحددت حقوقًا صريحة للأفراد، مع إقرار جزاءات رادعة للشركات المخالفة (Khalid، 2020). وهو ما يجعل المواءمة بين التشريعات الوطنية والمبادئ الدولية ضرورة أساسية، ليس فقط من أجل تعزيز حماية الأفراد، بل أيضًا لمواجهة التحديات العابرة للحدود التي يفرضها الفضاء الرقمي، حيث لم تعد البيانات مقيدة بالحدود الجغرافية وإنما أصبحت تتنقل بحرية بين الدول والشركات في إطار اقتصاد عالمي متشابك.

أهداف الدراسة

تهدف هذه الدراسة إلى تقديم معالجة علمية متعمقة لموضوع الحماية الإدارية للبيانات الشخصية من خلال مقارنة التشريعات الوطنية في الإمارات ومصر بالمبادئ الدولية للحوكمة. وقد جاءت الأهداف لتغطي ثلاثة مستويات مترابطة:

- **المستوى النظري** :توضيح الإطار المفاهيمي للبيانات الشخصية، والخصوصية، والحماية الإدارية، وإبراز جذورها في الفكر القانوني المعاصر، وذلك من أجل سد فجوة معرفية في الأدبيات العربية التي غالبًا ما ركزت على الحماية الجنائية أو المدنية.
- **المستوى التشريعي** :تحليل النصوص القانونية الوطنية في الإمارات ومصر، وبيان مدى شمولها وفعاليتها في حماية الأفراد من الانتهاكات الرقمية، مع تحديد أوجه التشابه والاختلاف مع النظام الأوروبي (GDPR) باعتباره النموذج الأبرز عالميًا.

- **المستوى العملي/التطبيقي** :تقييم دور الأجهزة الإدارية والجزاءات الرقابية في إنفاذ القوانين الوطنية، واستكشاف العقبات التي تواجهها في التطبيق، وصولًا إلى صياغة توصيات عملية يمكن أن تسهم في تطوير السياسات العامة (Hussein، 2020) فعالية الحماية.

من خلال هذه الأهداف، تسعى الدراسة إلى بناء جسر بين النصوص الوطنية والمعايير الدولية، بما يعزز من مكانة الحماية الإدارية كأحد أعمدة الحوكمة الرشيدة في البيئة الرقمية الحديثة (Al-Bustani، 2025؛ Ibrahim، 2025؛ Al-Hinai، 2025).

أسئلة الدراسة

تنبع أسئلة الدراسة من الإشكالية المركزية المتعلقة بمدى كفاية التشريعات الوطنية لحماية البيانات في مواجهة التحديات الرقمية الحديثة. ويمكن صياغة الأسئلة الرئيسة كما يلي:

1. إلى أي مدى نجحت التشريعات الوطنية في الإمارات ومصر في توفير حماية إدارية فعالة للبيانات الشخصية تتماشى مع معايير الحوكمة الدولية؟
2. كيف انعكست مبادئ الحوكمة مثل الشفافية، المساءلة، العدالة، والمساواة في نصوص هذه التشريعات، وهل وجدت طريقها إلى التطبيق العملي داخل المؤسسات؟
3. ما مدى فعالية الأجهزة الإدارية والجزاءات التنظيمية في فرض الامتثال؟ وما أبرز التحديات التي تواجهها في الواقع العملي؟
4. ما أوجه التشابه والاختلاف بين التجربتين الإماراتية والمصرية والتجربة الأوروبية(GDPR) ، وما الدروس التي يمكن الاستفادة منها لتطوير التشريعات العربية؟

هذه الأسئلة لا تسعى فقط إلى توصيف الواقع، بل تهدف إلى إنتاج تحليل نقدي معمق يساعد على صياغة حلول وتوصيات عملية. فهي تعكس انتقال البحث من مجرد رصد النصوص إلى اختبار فعاليتها في الواقع، وهو ما يميز هذه الدراسة عن غيرها من الدراسات الوصفية (Mahmoud، 2022؛ Khalid، 2020).

مفاهيم ومصطلحات الدراسة

تعريف البيانات الشخصية

تذهب الأدبيات القانونية الحديثة إلى أن البيانات الشخصية هي "كل معلومة تتعلق بشخص طبيعي معرف أو قابل للتعريف، سواء بشكل مباشر أو غير مباشر، وبأي وسيلة كانت" (Ibrahim، 2025). ويشمل ذلك الاسم، العنوان، رقم الهوية، المعطيات الصحية، المالية، والبيومترية، بالإضافة إلى البيانات الرقمية التي تنتج عن التفاعل عبر الإنترنت مثل عناوين بروتوكولات الإنترنت (IP) أو ملفات تعريف الارتباط. ويتميز هذا التعريف بشموليته وقدرته على استيعاب التطور التكنولوجي، إذ لم يعد قاصرًا على البيانات التقليدية بل أصبح يغطي البيانات المولّدة آليًا من

خلال الذكاء الاصطناعي وتقنيات إنترنت الأشياء. وقد تبنّت التشريعات الدولية مثل اللائحة الأوروبية العامة لحماية البيانات (GDPR) تعريفًا مشابهًا، ما يعكس وجود توجه عالمي نحو توحيد مفهوم البيانات الشخصية كمدخل لضمان الحماية القانونية لها. في السياق العربي، يعد هذا التعريف حديثًا نسبيًا، إذ لم تدخل معظم التشريعات العربية في تفاصيل دقيقة للبيانات الرقمية إلا خلال العقد الأخير.

تعريف الحماية الإدارية للبيانات الشخصية

تُعرف الحماية الإدارية بأنها "مجموعة التدابير الرقابية والتنظيمية التي تقوم بها السلطات الإدارية المختصة لضمان احترام التشريعات الخاصة بحماية البيانات، بما يشمل الرقابة المسبقة واللاحقة وتوقيع الجزاءات الإدارية" (Al-Rashed، 2020). ويميز هذا التعريف الحماية الإدارية عن الحماية المدنية أو الجنائية بتركيزه على الدور المؤسسي الوقائي للإدارة في ضمان الامتثال. ففي حين تسعى الحماية الجنائية إلى معاقبة المعتدي بعد وقوع الضرر، والحماية المدنية

إلى تعويض المتضرر، فإن الحماية الإدارية تركز على منع الانتهاكات قبل حدوثها عبر أدوات الرقابة والردع الإداري. وقد تبنت أنظمة عربية مثل القانون المصري رقم 151 لسنة 2020 هذا النهج من خلال إنشاء "مركز حماية البيانات الشخصية" كسلطة رقابية، بينما سارت الإمارات في اتجاه مشابه عبر تأسيس "مكتب حماية البيانات" بموجب المرسوم بقانون اتحادي رقم 45 لسنة 2021. إن هذا الدور الإداري يعكس بوضوح فلسفة الحوكمة الحديثة التي تضع المؤسسات التنظيمية المستقلة في قلب عملية حماية الحقوق الرقمية.

تعريف الحق في الخصوصية

يشير الحق في الخصوصية إلى "حرمة الحياة الخاصة وحماية البيانات الفردية من أي تدخل تعسفي من الأفراد أو الدولة، وجعلها من الحقوق الدستورية التي لا يجوز المساس بها" (Wajdi، 2018). ويُعتبر هذا الحق من أقدم الحقوق التي ارتبطت بالفكر الليبرالي وحقوق الإنسان منذ القرن التاسع عشر، حيث بدأ مع حق الإنسان في أن يُترك وشأنه (The right to be let alone) ليتطور لاحقًا إلى حماية أشمل تشمل البيانات الشخصية والمراسلات الإلكترونية. وتؤكد المواثيق الدولية مثل الإعلان العالمي لحقوق الإنسان (1948) والعهد الدولي للحقوق المدنية والسياسية (1966) على هذا الحق باعتباره ضمانة أساسية لحرية الفرد وكرامته. وتُظهر التجربة الأوروبية، خاصة أحكام المحكمة الأوروبية لحقوق الإنسان، كيف تحول هذا المفهوم إلى ركيزة قانونية ملزمة تمنع أي تدخل غير مشروع في الحياة الخاصة. أما في السياق العربي، فإن حماية الخصوصية بدأت تظهر تدريجيًا في الدساتير والتشريعات الحديثة، لتواكب التحديات المتزايدة في الفضاء الرقمي وتتصدى لجرائم اختراق الحسابات وسرقة البيانات.

تعريف الحوكمة في مجال البيانات

تُعرف الحوكمة الرقمية بأنها "إخضاع الجهات التي تجمع أو تعالج البيانات لمبادئ المساءلة، الشفافية، العدالة، والمساواة، بما يضمن حماية الأفراد من التمييز وسوء الاستغلال" (Al-Taie، 2022). ويعكس هذا التعريف التوسع في مفهوم الحوكمة ليشمل البعد الرقمي إلى جانب البعد المالي والإداري التقليدي. ففي ضوء التحول الرقمي، لم يعد كافيًا الحديث عن رقابة مالية أو مساءلة سياسية، بل أصبح من الضروري وضع آليات مؤسسية تضمن الاستخدام الأخلاقي والمسؤول للبيانات. ويُلاحظ أن هذا التعريف مستلهم من مبادئ الحوكمة العالمية التي طرحتها منظمات مثل البنك الدولي ومنظمة التعاون الاقتصادي والتنمية(OECD) ، والتي تؤكد على أهمية الشفافية والمساءلة في بناء الثقة بين الدولة والمجتمع. وفي السياق المحلي، بدأت بعض التشريعات الوطنية تتبنى هذا المنظور، من خلال فرض التزامات على المؤسسات لنشر سياسات حماية البيانات، وتعيين مسؤول لحماية البيانات(DPO) ، وتقديم تقارير دورية حول أنشطة المعالجة. وهكذا تتحول الحوكمة من إطار نظري إلى آلية عملية لحماية الأفراد وتطوير الإدارة العامة في البيئة الرقمية.

الدراسات السابقة

تشير مراجعة الدراسات السابقة إلى وجود اهتمام متزايد في الأدبيات العربية والأجنبية بموضوع حماية البيانات، لكن مع تباين في الزوايا التي عولج منها الموضوع. فقد ركزت بعض الدراسات على **الحماية الجنائية**، مثل دراسة Al-Qatatsha (2022) التي بينت أهمية العقوبات الجنائية في مواجهة جرائم إساءة استخدام البيانات، وكذلك دراسة Al-Barwani (2022) التي تناولت الجزاءات الإدارية لكنها ركزت على بعدها العقابي دون التوسع في البنية المؤسسية. أما الدراسات المدنية، مثل دراسة Abu Khumra (2021)، فقد تناولت التعويضات كوسيلة لحماية الأفراد بعد وقوع الضرر.

في المقابل، سلطت بعض الدراسات الضوء على البعد الدستوري والحقوقي، مثل دراسة Hussein (2020) التي أبرزت ارتباط حماية البيانات بالحق في الخصوصية كأحد حقوق الإنسان، ودراسة Khalid (2020) التي حللت اللائحة الأوروبية (GDPR) بوصفها النموذج الأكثر صرامة عالميًا. كما جاءت دراسات حديثة مثل دراسة Al-Bustani (2025) وIbrahim (2025) لتؤكد أهمية البعد الإداري والمؤسسي في الحماية، وهو البعد الذي ظل مهمشًا نسبيًا في الأدبيات العربية.

من خلال استقراء هذه الدراسات، يتضح أن ثمة فجوة معرفية تتمثل في ضعف الدراسات المقارنة التي تجمع بين التشريعات الوطنية العربية والمعايير الدولية من منظور إداري مؤسسي. وهنا تبرز أهمية هذه الدراسة باعتبارها محاولة جادة لملء هذه الفجوة، من خلال الجمع بين التحليل التشريعي، والتقييم المؤسسي، والمقارنة الدولية، بما يعزز من القيمة العلمية والعملية للبحث (Osman، 2025؛ Al-Hinai، 2025).

موقع الدراسة في الأدبيات القانونية

عند مراجعة الأدبيات القانونية، يتبين أن معظم الدراسات العربية تناولت موضوع حماية البيانات إما من زاوية القانون الجنائي، مركزة على الجرائم الإلكترونية والعقوبات الجنائية (Al-Qatatsha، 2022؛ Al-Barwani، 2022)، أو من منظور القانون المدني، متناولة المسؤولية المدنية عن التعدي على البيانات (Osman، 2025؛ Abu Khumra، 2021). في حين أن الدراسات التي أولت عناية خاصة بالجانب الإداري لا تزال محدودة نسبياً. وعلى الرغم من وجود بعض الأبحاث التي لامست هذا الجانب، مثل تلك التي بحثت في دور القضاء الإداري في حماية البيانات أو سلطات المراكز التنظيمية (Al-Hinai، 2025)، إلا أن الحاجة ما تزال قائمة لدراسات معمقة تستكشف العلاقة بين الحماية الإدارية للبيانات والمبادئ الدولية للحوكمة، وهو ما يسعى هذا البحث إلى معالجته من خلال منهج مقارن بين التجربتين الإماراتية والمصرية، مع إسقاطات على المعايير الدولية ذات الصلة (Al-Bustani، 2025).

مراجعة الأدبيات

أولاً: الدراسات ذات الطابع الجنائي

تناولت العديد من الدراسات موضوع حماية البيانات الشخصية من منظور القانون الجنائي، حيث ركزت على الأفعال الإجرامية التي تستهدف البيانات، والعقوبات المقررة لمواجهتها. فقد أوضحت دراسة Al-Qatatsha (2022) أن حماية البيانات الرقمية تتطلب تقسيمها إلى جانبين أساسيين: الحماية الموضوعية التي تركز على الجرائم المتمثلة في مخالفة شروط المعالجة أو إساءة استخدامها، والحماية الإجرائية التي تشمل مراحل التحقيق بمختلف درجاتها، من التحقيق الابتدائي إلى المحاكمة النهائية. ويكشف هذا التقسيم عن محاولة جادة لفهم الأبعاد العملية للجريمة المعلوماتية، لكنه يبقى بعيداً عن تناول الدور الإداري الوقائي.

أما دراسة Al-Barwani (2022)، فقد تعمقت في الحماية الجزائية للبيانات الشخصية من خلال تقسيمها إلى جرائم واقعة على البيانات (كالاستيلاء غير المشروع، أو التلاعب في البيانات) وجرائم لاحقة لمعالجتها. وأكدت الدراسة أن النصوص العقابية ضرورية لردع المخالفين، غير أن الاعتماد المفرط على الجزاء الجنائي دون تفعيل آليات إدارية مساندة قد يؤدي إلى قصور في حماية الأفراد بشكل يومي.

وتذهب دراسة Hussein (2020) إلى أن معالجة البيانات الشخصية آلياً تفتح المجال لجرائم متعددة مثل إساءة استخدام السلطة من قبل المسؤول عن المعالجة، أو التعدي على حقوق الأشخاص في الخصوصية، وقد تناولت الدراسة ذلك من خلال مقارنة بين التشريعات العربية والأجنبية. بينما أوضح Khalid (2020) أن الجرائم

الإلكترونية المرتبطة بالبيانات الشخصية تتطلب مزيجاً من الحماية التشريعية والإدارية، وأن الاقتصار على العقوبة الجنائية قد لا يحقق الردع الكافي في ظل اتساع نطاق الجرائم العابرة للحدود.

يُلاحظ أن هذه الدراسات مجتمعة قدمت إطاراً جنائياً متيناً لحماية البيانات، لكنها أهملت أو قللت من شأن دور المؤسسات الإدارية، مكتفية بالحديث عن العقوبات والجزاءات الجنائية دون الغوص في السياسات الوقائية أو آليات الرقابة الإدارية.

ثانياً: الدراسات ذات الطابع المدني

تُبرز الدراسات المدنية جانباً آخر من الحماية يتمثل في العلاقة القانونية بين الأفراد ومزوّدي الخدمة. فقد ركز Osman (2025) على أن البيانات الشخصية تعد جزءاً من الحقوق اللصيقة بالشخصية، ومن ثم فهي تستوجب حماية مدنية عبر إقرار حق الشخص في الاطلاع على بياناته أو محوها، بل ومساءلة المتسبب في انتهاكها. وتظهر أهمية هذا الطرح في كونه يعترف بحق الأفراد في التحكم في بياناتهم، لكنه لا يقدم تفصيلاً كافياً لدور الأجهزة الإدارية في ضمان ممارسة هذا الحق.

أما Abu Khumra (2021) فقد ركزت على المسؤولية المدنية الناشئة عن التعدي على البيانات عبر الإنترنت، مفرقة بين المسؤولية العقدية التي تقوم على إخلال مزوّد الخدمة بالتزاماته، والمسؤولية التقصيرية الناشئة عن الاعتداء غير المشروع على البيانات. وتؤكد هذه الدراسة أن القضاء المدني يلعب دوراً محورياً في تعويض الأضرار الناتجة عن انتهاك الخصوصية، إلا أن التعويض بعد وقوع الضرر لا يغني عن الحاجة إلى حماية وقائية وإدارية استباقية.

وتكشف هذه الدراسات أن الحماية المدنية رغم أهميتها، تظل ذات طبيعة علاجية أكثر من كونها وقائية، وأنها لا تعوض عن غياب الأجهزة الإدارية القادرة على التدخل السريع لمنع الانتهاكات قبل وقوعها.

ثالثاً: الدراسات ذات الطابع الدستوري

ركزت بعض الأدبيات على التأصيل الدستوري لحماية البيانات باعتبارها جزءاً من الحقوق الأساسية. فقد أوضح Mahmoud (2022) أن الدساتير الحديثة، مثل الدستور المصري لعام 2014، كفلت حماية البيانات الشخصية عبر نصوص واضحة، مثل المادة (68) التي نصت على أن المعلومات والبيانات ملك للشعب، وأن الدولة تلتزم بحمايتها. كما أشار إلى أن القضاء الدستوري في فرنسا ومصر لعب دوراً مهماً في تعزيز هذه الحماية من خلال الرقابة على القوانين واللوائح.

وتذهب هذه الدراسة إلى أن النصوص الدستورية تمثل الإطار الأعلى للحماية، لكنها بحاجة إلى أدوات تنفيذية، أبرزها الأجهزة الإدارية المختصة. ومن ثم، فإن الدستور يضع الأساس، بينما يظل تفعيل الحماية متوقفاً على التشريعات والآليات الإدارية.

ويلاحظ هنا أن التأصيل الدستوري للحماية يبرز الطابع المبدئي للحق في الخصوصية، لكنه لا يحدد تفاصيل التنفيذ. وهذه الفجوة تجعل البحث في الحماية الإدارية أمراً ضرورياً لاستكمال البناء الدستوري.

رابعاً: الدراسات المقارنة

ساهمت الدراسات المقارنة في إبراز التنوع بين النظم القانونية المختلفة. فقد تناول Al-Hinai (2025) القوانين المقارنة لحماية البيانات في الدول العربية والأجنبية، موضحاً التطور التاريخي لهذه التشريعات والاختلاف في آليات الرقابة والعقوبات. وخلص إلى أن الدول التي اعتمدت على أجهزة إدارية متخصصة، مثل سلطات حماية البيانات في الاتحاد الأوروبي، كانت أكثر نجاحاً في تطبيق القوانين.

أما Hussein (2020) فقد ركز على التجارب الأجنبية في الحماية الجنائية للبيانات، مبرزاً كيف أن بعض الأنظمة اكتفت بتجريم الأفعال، بينما تبنت أخرى مزيجاً من العقوبات والآليات الإدارية. ومن جانبه، أوضح Khalid (2020) أن الحماية الفعالة لا تتحقق إلا من خلال توازن بين التشريعات الوطنية والمعايير الدولية مثل GDPR.

وتكشف هذه الدراسات أن التجربة الأوروبية، بخاصة في إطار الاتحاد الأوروبي، تمثل نموذجاً رائداً في دمج الحماية التشريعية مع الحماية الإدارية، وهو ما تفتقر إليه العديد من الأنظمة العربية.

خامساً: الدراسات ذات الطابع الإداري

تُعد الدراسات التي تناولت الحماية الإدارية للبيانات الشخصية نادرة نسبياً في الأدبيات العربية. إلا أن Al-Bustani (2025) قدّم دراسة متميزة ركزت على دور الإدارة في حماية البيانات في كل من الإمارات ومصر. وأبرزت الدراسة أهمية الأجهزة الإدارية مثل "مركز حماية البيانات الشخصية" في مصر و"مكتب حماية البيانات" في الإمارات، موضحة اختصاصاتها في منح التراخيص، مراقبة الامتثال، وتوقيع الجزاءات الإدارية.

كما أشار Ibrahim (2025) إلى أن المعالجة الآلية للبيانات لا يمكن أن تظل مجرد شأن تقني، بل تحتاج إلى إشراف إداري يضمن التزام المؤسسات بالمعايير القانونية. وأكدت الدراسة على ضرورة تعزيز قدرات الأجهزة الإدارية بالتقنيات الحديثة لمواكبة التطورات المتسارعة.

وتوضح هذه الدراسات أن الحماية الإدارية تمثل خط الدفاع الأول ضد الانتهاكات، كونها قادرة على التدخل السريع وفرض الجزاءات دون الحاجة إلى إجراءات قضائية مطولة. لكنها أيضاً تواجه تحديات مثل ضعف الموارد البشرية، غياب التنسيق بين الجهات، وتعارض الحماية مع بعض الاعتبارات الأمنية.

سادساً: المقارنة النقدية بين الاتجاهات

عند النظر إلى الدراسات السابقة بشكل تكاملي، نجد أن الاتجاه الجنائي ركز على الردع عبر العقوبة، والمدني ركز على التعويض بعد وقوع الضرر، والدستوري ركز على النصوص المبدئية، بينما المقارن أبرز تنوع التجارب. أما الإداري، فرغم محدودية الأدبيات فيه، فإنه يقدم البعد الأكثر واقعية وفعالية في حماية البيانات.

ويكشف هذا التحليل أن دمج الأبعاد المختلفة (جنائية، مدنية، دستورية) في إطار إداري منظم هو السبيل لتحقيق حماية شاملة للبيانات الشخصية.

سابعاً: الفجوات البحثية

يتضح أن معظم الدراسات السابقة لم تمنح الحماية الإدارية ما تستحقه من اهتمام، وأن هناك فجوة واضحة تتمثل في قلة البحوث التي تربط بين الحماية الإدارية والمبادئ الدولية للحوكمة. فالمساءلة والشفافية والمساواة ليست مجرد قيم مجردة، بل يمكن ترجمتها إلى آليات إدارية عملية مثل نشر التقارير السنوية عن الانتهاكات، إنشاء منصات للشكاوى الإلكترونية، وتفعيل الرقابة على القطاع الخاص. ومن هنا، يهدف هذا البحث إلى سد هذه الفجوة من خلال دراسة مقارنة بين التشريعات الوطنية (الإمارات ومصر) والمبادئ الدولية، مع التركيز على الكيفية التي تتولاها الإدارة في حماية البيانات الشخصية.

المنهجية

الأساس الفلسفي للمنهجية

تستند هذه الدراسة إلى رؤية علمية تعتبر أن البحث القانوني والإداري في مجال حماية البيانات الشخصية لا يمكن أن يقتصر على مجرد رصد النصوص أو استعراض الأحكام القضائية، وإنما يتطلب إطارًا منهجيًا يدمج بين القانون والحوكمة والإدارة العامة. فالبيانات الشخصية تُعد اليوم مورداً استراتيجياً يعادل في قيمته الموارد التقليدية للدول، ما يفرض منهجية علمية دقيقة قادرة على تحليل القوانين، مقارنتها، وتقييم أدائها المؤسسي (Al-Bustani، 2025؛ Ibrahim، 2025).

طبيعة المنهج المعتمد

اعتمدت الدراسة **المنهج المقارن التحليلي** كمنهج رئيسي، لأنه يتيح:

- تحليل النصوص القانونية الوطنية (الإماراتية والمصرية).
- مقارنتها مع المعايير الدولية مثل GDPR الأوروبي.
- استجلاء أوجه التشابه والاختلاف، وقياس مدى التوافق مع مبادئ الحوكمة الدولية (Al-Hinai، 2025؛ Hussein، 2020).

كما تم استخدام **المنهج الوصفي التحليلي** كمنهج مكمل، لتوصيف المفاهيم القانونية (الخصوصية، البيانات، الحماية الإدارية) ثم تحليلها نقدياً. ويُضاف إلى ذلك توظيف **المقاربة المؤسسية النقدية** لتقييم أداء الأجهزة الإدارية، باعتبارها الفاعل المركزي في إنفاذ التشريعات (Osman، 2025؛ Al-Barwani، 2022).

مبررات اختيار هذه المنهجية

1 قصور المناهج التقليدية

- **المنهج الجنائي** :يركز على العقوبات لكنه يغفل الوقاية الإدارية (Al-Qatatsha، 2022).

- **المنهج المدني** :يعالج التعويض بعد وقوع الضرر، دون منع الانتهاكات مسبقاً (Abu Khumra، 2021).
- **المنهج الدستوري** :يؤسس الحق نظريًا، لكنه لا يوفر آليات عملية للتنفيذ (Mahmoud، 2022).

2. الحاجة إلى المقارنة

نظرًا للطبيعة العابرة للحدود للبيانات، فإن أي دراسة وطنية بمعزل عن المعايير الدولية تكون ناقصة. ومن هنا تأتي أهمية المنهج المقارن الذي يسمح بتقدير مدى اقتراب التجارب الوطنية من النماذج الدولية الرائدة (Khalid، 2020).

3. ارتباط المنهجية بأهداف البحث

لأن أحد أهداف البحث هو **تقييم دور الأجهزة الإدارية** في حماية البيانات، كان لا بد من تبني منهجية تستند إلى تحليل مؤسسي نقدي يقيس الأداء الفعلي لهذه الأجهزة (Al-Bustani، 2025).

مجتمع البحث ومصادره

يستند هذا البحث إلى مزيج من المصادر الأولية والثانوية التي توفر قاعدة معرفية ومنهجية متينة للتحليل المقارن. فمن ناحية، تشكل القوانين الوطنية الخاصة بحماية البيانات في كل من الإمارات ومصر الركيزة الأساسية للمصادر الأولية، إذ تُمثل النصوص التشريعية المرجع المباشر لفهم الإطار القانوني المنظم للبيانات الشخصية، إلى جانب النصوص الدستورية ذات الصلة التي تعكس البعد الحقوقي الأوسع، فضلاً عن القرارات التنفيذية واللوائح التنظيمية التي تحدد آليات تفعيل تلك القوانين على أرض الواقع. ومن ناحية أخرى، تُستكمل هذه المصادر بمجموعة من الأدبيات الثانوية التي أغنت النقاش العلمي، حيث تضمنت الدراسات الأكاديمية المتخصصة التي تناولت أبعاد الحماية الإدارية في السياق العربي (Osman، 2025؛ Abu Khumra، 2021؛ Al-Barwani، 2022؛ Al-Qatatsha، 2022)، إضافة إلى الأدبيات المقارنة التي سلطت الضوء على التجربة الأوروبية والدولية بوصفها نموذجًا متقدماً في مجال حماية البيانات (Al-Hinai، 2025؛ Hussein، 2020؛ Khalid، 2020). كما اعتمد البحث على الوثائق والتقارير الدولية الصادرة عن منظمات أممية وإقليمية مثل إرشادات الأمم المتحدة ومنظمة التعاون الاقتصادي والتنمية، وذلك لتعزيز البعد المعياري والحوكمي وربط التشريعات الوطنية بالإطار الدولي الأشمل. وبهذا التداخل بين المصادر القانونية الوطنية والأدبيات العلمية والدولية، يضمن البحث تكوين صورة شاملة تسمح بإجراء تحليل مقارن متوازن يجمع بين النصوص النظرية والتطبيقات العملية.

أدوات وتقنيات البحث

1. **التحليل النصي** :دراسة المصطلحات القانونية المستخدمة في القوانين الوطنية، مثل تعريف "المعالجة"، "المتحكم"، و"البيانات الحساسة."

2. **التحليل المعياري** :وضع النصوص الوطنية في مواجهة نصوص GDPR لمعرفة أوجه القوة والقصور.
3. **التحليل المؤسسي** :فحص البنية القانونية والتنظيمية للأجهزة الإدارية، ومدى استقلاليتها وكفاءتها (Ibrahim، 2025).
4. **التحليل النقدي المقارن** :مقارنة الجزاءات الإدارية في الإمارات ومصر (الإنذار، الغرامة، وقف الترخيص) بالجزاءات المقررة دولياً، وتقييم فعاليتها (Al-Barwani، 2022).

نطاق البحث وحدوده

ينحصر نطاق هذا البحث في معالجة البعد الإداري لحماية البيانات الشخصية، إذ يركز على دراسة الأطر القانونية والتنظيمية والرقابية التي وضعتها السلطات الوطنية في كل من الإمارات ومصر، دون التطرق بشكل مباشر إلى الجوانب التقنية البحتة المرتبطة بأمن الشبكات أو الحلول البرمجية. ويعود هذا التحديد الموضوعي إلى أن الهدف الأساسي من الدراسة يتمثل في تقييم فعالية الأدوات الإدارية والمؤسسية في فرض الامتثال وحماية الحقوق، وهو ما يميزها عن الدراسات ذات الطابع التكنولوجي البحت التي تنصب على تقنيات التشفير أو أنظمة الحماية الإلكترونية. وبهذا التحديد، ينصرف البحث إلى إبراز الدور المركزي للإدارة العامة في حماية البيانات بوصفها أحد أبعاد الحوكمة الرشيدة.

أما من الناحية الجغرافية، فقد اختار البحث الاقتصار على نموذجين عربيين هما الإمارات ومصر، وذلك بالنظر إلى الريادة التشريعية التي حققتها الدولتان في مجال سن قوانين خاصة بحماية البيانات الشخصية خلال السنوات الأخيرة. فالإمارات تبنت المرسوم بقانون اتحادي رقم (45) لسنة 2021، في حين أقرت مصر القانون رقم (151) لسنة 2020، وهو ما جعلهما من أوائل الدول العربية التي وضعت أطرًا قانونية متكاملة في هذا المجال. ويتيح هذا الاختيار إمكان إجراء مقارنة ثرية بين تجربتين عربيتين مختلفتين من حيث السياق المؤسسي والتشريعي، وفي الوقت نفسه متقاربتين من حيث الهدف المتمثل في مواءمة التشريعات الوطنية مع المعايير الدولية.

أما على الصعيد الزمني، فإن البحث يغطي الفترة الممتدة من عام 2020 إلى عام 2025، وهي فترة ذات دلالة خاصة لأنها شهدت صدور أبرز القوانين الوطنية الخاصة بحماية البيانات في الدولتين، إضافة إلى تزايد النقاش الدولي حول قضايا الخصوصية وحماية المعلومات في ظل الطفرة الرقمية المتسارعة. وقد اختير هذا الإطار الزمني بدقة ليعكس مرحلة التحول من غياب شبه كامل للتشريعات إلى وجود منظومات قانونية ومؤسساتية حديثة، بما يسمح بدراسة النصوص وتقييم آثارها العملية في السنوات الأولى لتطبيقها.

الصدق العلمي والموضوعية

يرتكز هذا البحث على الالتزام بالصدق العلمي والموضوعية باعتبارهما من أهم معايير الدراسات الأكاديمية الرصينة. وقد جرى تحقيق ذلك من خلال الاعتماد على مصادر متعددة ومتنوعة شملت النصوص التشريعية الوطنية في الإمارات ومصر، والدراسات الأكاديمية المتخصصة، فضلًا عن الوثائق والمعايير الدولية ذات الصلة بمجال حماية

البيانات والحوكمة. إن هذا التنوع في المصادر يعكس حرص الباحث على تقديم صورة متوازنة للموضوع، وتفادي الانحياز إلى اتجاه واحد بعينه.

كما تميز البحث باعتماده على المقارنة النقدية بين اتجاهات مختلفة، حيث لم يقتصر على استعراض التشريعات الوطنية فحسب، بل وضعها في مواجهة المرجعيات الدولية وأحكام القضاء المقارن، مع تقديم قراءة تحليلية موضوعية تسعى إلى الكشف عن أوجه القوة والقصور في كل اتجاه (Hussein، 2020؛ Osman، 2025). وبهذا، يسعى البحث إلى بناء طرح علمي متوازن لا يكتفي بعرض الآراء، وإنما يتجاوزها إلى مناقشتها واستخلاص دلالاتها.

وإلى جانب ذلك، اعتمد البحث على الاستدلال بالنصوص القانونية والتجارب الواقعية في كل من الإمارات ومصر، وهو ما أضفى على نتائجه قدرًا أكبر من المصداقية والموضوعية، بخلاف الدراسات التي تقتصر على الطرح النظري أو التحليل المجرد (Al-Hinai، 2025). وبهذا الأسلوب، استطاع البحث أن يجمع بين العمق النظري والتطبيق العملي، بما يضمن نتائج علمية يمكن الاعتماد عليها في تطوير السياسات العامة وتعزيز الحماية الإدارية للبيانات الشخصية.

القيمة العلمية والإضافة الجديدة

هذه المنهجية تقدم قيمة مضاعفة لأنها:

- تدمج بين المناهج الوصفية والمقارنة والتحليل المؤسسي.
- تعالج فجوة معرفية حول الحماية الإدارية للبيانات الشخصية.
- تقدم نتائج قابلة للتطبيق عبر سياسات عامة واضحة.
- تربط بين الحماية الوطنية والحوكمة الدولية في إطار شامل (Al-Bustani، 2025؛ Mahmoud، 2022).

النتائج والتحليل

أولاً: شمولية وعمق التشريعات الوطنية

أظهرت نتائج التحليل أن الإمارات ومصر تبنّتا خلال السنوات الأخيرة منظومتين قانونيتين لحماية البيانات الشخصية تعكسان رغبة جادة في الانضمام إلى الحراك العالمي الرامي إلى تكريس الخصوصية كحق أساسي، لكنهما اختلفتا من حيث العمق والتفصيل. فقد جاء المرسوم بقانون اتحادي رقم (45) لسنة 2021 في الإمارات ليضع نصوصًا دقيقة تُعرّف المصطلحات الجوهرية، وتُحدّد بدقة العلاقة بين المتحكم بالبيانات والمعالج لها، وتقرّ حقوقًا فردية واسعة للأشخاص مثل الحق في التصحيح، والحق في المحو، والحق في الاعتراض على بعض أشكال المعالجة (Al-Bustani، 2025). ويمثل هذا التشريع نقلة نوعية في النظام القانوني الإماراتي لأنه يقترب كثيرًا من فلسفة التشريع الأوروبي (GDPR) القائم على حماية الحقوق الفردية أولاً ثم وضع التزامات مؤسسية ثانياً.

أما في مصر، فقد جاء القانون رقم (151) لسنة 2020 ليؤسس منظومة إدارية مركزية عبر "مركز حماية البيانات الشخصية". ورغم أن القانون تضمن نصوصًا تُعنى بالحقوق الفردية، إلا أن التركيز الأكبر كان على صلاحيات المركز ودوره في الرقابة والترخيص وإصدار اللوائح. هذا التوجه يعكس فلسفة تشريعية مختلفة، إذ يتمحور حول الإدارة المركزية أكثر من تمحوره حول تمكين الأفراد (Mahmoud، 2022). وهنا يتضح أن المقاربة الإماراتية أقرب إلى منح الأفراد أدوات قانونية مباشرة، بينما المقاربة المصرية أقرب إلى "الحماية عبر المؤسسة". وقد أثار هذا التباين تساؤلات حول أي النموذجين أكثر قدرة على حماية الأفراد عمليًا: النموذج الذي يثقّف الأفراد ويعطيهم أدوات، أم النموذج الذي يركّز على جهاز إداري قوي يحتكر صلاحية التدخل (Ibrahim، 2025؛ Osman، 2025).

ثانياً: فعالية الأجهزة الإدارية ومحدودية الاستقلالية

أظهرت النتائج أن الأجهزة الإدارية المنشأة في كل من الإمارات ومصر تمثل حجر الأساس في تطبيق النصوص، غير أن فعاليتها تختلف من حيث الاستقلالية والكفاءة. ففي الإمارات، أُنشئ "مكتب حماية البيانات" ليكون جهازًا رقابيًا وتنظيميًا يتابع تنفيذ القانون. وقد منح المشرع هذا المكتب سلطات تشمل إصدار التراخيص، مراقبة الامتثال، فرض الجزاءات، بل وإصدار التوجيهات الملزمة للقطاع الخاص (Al-Hinai، 2025). غير أن تبعيته للسلطة التنفيذية تحد من استقلاليته، مما قد يؤدي إلى تضارب محتمل بين متطلبات حماية البيانات ومصالح حكومية أخرى. وفي مصر، مثّل إنشاء "مركز حماية البيانات الشخصية" خطوة مهمة لأنه أول جهاز إداري متخصص على مستوى الدولة العربية يُمنح صلاحيات قانونية واسعة النطاق. ومع ذلك، تُظهر الممارسة أن المركز يواجه عدة تحديات أبرزها ضعف الكوادر الفنية المؤهلة لمتابعة جميع أشكال المعالجة الرقمية للبيانات، إضافة إلى محدودية قدراته المالية والفنية (Al-Barwani، 2022). كما أن المركز يجد صعوبة في مراقبة الشركات الدولية الكبرى التي تتعامل مع كميات هائلة من البيانات وتتمتع بقدرة تفاوضية عالية.

تكشف هذه النتائج أن فعالية الأجهزة الإدارية لا تتحدد فقط بما يُمنح لها من صلاحيات قانونية، وإنما أيضًا بمدى استقلاليتها عن السلطة التنفيذية، وبقدرتها على استقطاب كوادر مؤهلة في القانون والتقنية والإدارة. فالمؤسسة الإدارية التي تفتقر إلى هذه الاستقلالية ستبقى معرضة للتأثيرات السياسية، بينما المؤسسة التي تفتقر إلى الكوادر ستتحول إلى جهاز صوري عاجز عن فرض القانون (Al-Qatatsha، 2022).

ثالثاً: جدوى الجزاءات الإدارية وقدرتها على الردع

تؤكد النتائج أن الجزاءات الإدارية تُعد وسيلة أساسية لضمان الامتثال، غير أن تقييم فعاليتها يكشف عن فجوة واضحة بين التشريعات العربية والنموذج الأوروبي. ففي الإمارات، نص القانون على جزاءات تبدأ بالإنذار وتنتهي بوقف الترخيص أو حتى نشر بيانات المخالفين على الملأ كنوع من التشهير الإداري، وهو ما يشكل ضغطًا على المؤسسات المخالفة (Al-Bustani، 2025). أما في مصر، فقد منح القانون "المركز" صلاحية فرض غرامات مالية وسحب التراخيص عند الاقتضاء.

لكن عند المقارنة معGDPR ، يتضح أن النظام الأوروبي أكثر صرامة وفعالية، إذ تصل العقوبات إلى مبالغ ضخمة تعادل 20 مليون يورو أو 4% من الإيرادات العالمية للمؤسسة المخالفة (Khalid، 2020). هذه العقوبات جعلت من الامتثال ضرورة قصوى للشركات الأوروبية والعالمية العاملة في السوق الأوروبية. بينما تظل العقوبات في الإمارات ومصر أقل ردعًا، ما يجعل بعض المؤسسات تعتبرها "تكلفة محتملة" لا أكثر (Mahmoud، 2022؛ Abu Khumra، 2021). ويعني ذلك أن الحماية الإدارية لا تكتمل إلا إذا كانت الجزاءات ذات طبيعة تصاعدية، تتناسب مع حجم الضرر المحتمل، وتطبق بصرامة على جميع المؤسسات دون استثناء.

رابعاً: انعكاس مبادئ الحوكمة الدولية

أوضحت النتائج أن مبادئ الحوكمة الدولية، مثل المساءلة والشفافية والعدالة، قد انعكست جزئيًا في النصوص الوطنية، لكن التطبيق المؤسسي ظل محدودًا. ففي الإمارات، نص القانون على وجوب تعيين مسؤول حماية بيانات داخل المؤسسات الكبرى، وهو ما ينسجم مع مبدأ المساءلة، إلا أن آليات تقييم أداء هذا المسؤول أو محاسبته لم تُفصّل بعد (Ibrahim، 2025). وفي مصر، لم يُلزم القانون المؤسسات بتعيين مثل هذا المسؤول بشكل صريح، مما أضعف مستوى المساءلة الداخلية.

أما مبدأ الشفافية، فقد ظهر في النصوص التي توجب إبلاغ الأفراد بكيفية جمع بياناتهم وأغراض استخدامها، إلا أن غياب التقارير الدورية التي تعرض للرأي العام مدى التزام المؤسسات قلل من أثر هذا المبدأ. وفيما يتعلق بالعدالة والمساواة، فإن التشريعات نصّت على حماية شاملة لجميع الأفراد دون تمييز، لكن التحديات التقنية والمالية للمؤسسات الصغيرة تجعل قدرتها على الالتزام أضعف من المؤسسات الكبرى، ما يخلق نوعًا من التفاوت غير المقصود (Osman، 2025).

هذه النتائج تؤكد أن النصوص وحدها لا تكفي لتجسيد مبادئ الحوكمة، بل يجب أن تُترجم إلى ممارسات إدارية مؤسسية مدعومة بآليات رقابة صارمة، وهو ما لا يزال غائبًا في التطبيق العربي (Al-Hinai، 2025).

خامساً: الفجوة بين النصوص والتطبيق

أحد أبرز ما أظهره البحث هو وجود فجوة عميقة بين ما تنص عليه القوانين وما يجري في الواقع العملي. ففي الإمارات، ورغم وجود قانون متقدم، فإن العديد من المؤسسات لم تُعدّ أنظمتها الداخلية لتتماشى مع متطلبات الامتثال، سواء من حيث تدريب الموظفين أو تحديث البنية التحتية الرقمية. وهذا الضعف يعكس الحاجة إلى سياسات عامة داعمة لتسهيل الانتقال نحو الامتثال (Ibrahim، 2025). وفي مصر، ورغم إنشاء "مركز حماية البيانات"، فإن المركز يواجه صعوبة في فرض رقابته على جميع المؤسسات، ما يؤدي إلى تفاوت في مستوى الامتثال بين القطاعات الاقتصادية المختلفة (Mahmoud، 2022).

إن هذه الفجوة بين النصوص والتطبيق تمثل التحدي الأكبر أمام الحماية الإدارية، لأنها تُفقد النصوص قيمتها العملية، وتجعل القانون أقرب إلى "إعلان نوايا" أكثر من كونه أداة تنظيمية فعالة (Al-Barwani، 2022؛ Al-

Qatatsha، 2022). وتشير هذه النتائج إلى أن تطوير الحماية الإدارية يتطلب استراتيجيات متكاملة، تبدأ من بناء قدرات بشرية متخصصة، وتمر بتعزيز البنية التحتية التقنية، وتنتهي بتفعيل الرقابة الإدارية بشكل صارم ومتوازن.

سادساً: المقارنة النقدية مع التجربة الأوروبية

تكشف المقارنة مع GDPR أن الدول العربية، رغم تقدمها النسبي، لا تزال في مرحلة التأسيس مقارنة بالنموذج الأوروبي. فالأجهزة الأوروبية، مثل "هيئة حماية البيانات" الفرنسية (CNIL) أو الألمانية، تتمتع باستقلال مالي وإداري، وتعمل كهيئات شبه قضائية تصدر قرارات ملزمة لا يمكن إلغاؤها إلا عبر القضاء (Hussein، 2020). في المقابل، الأجهزة العربية لا تزال مرتبطة بالسلطة التنفيذية، مما يضعف من استقلاليتها.

كذلك فإن الجزاءات الأوروبية أكثر صرامة، بينما لا تزال العقوبات العربية في معظمها محدودة، وهو ما يقلل من فاعليتها كرادع. يضاف إلى ذلك أن GDPR وضعت آليات واضحة للتعاون الدولي، بحيث يتم تبادل المعلومات بين سلطات الحماية الأوروبية، بينما لا توجد مثل هذه الآليات بين الإمارات ومصر أو غيرهما من الدول العربية (Khalid، 2020؛ Al-Hinai، 2025). وتؤكد هذه الفوارق أن التشريعات العربية بحاجة إلى إصلاحات مؤسسية وهيكلية إذا أرادت أن تحقق مستوى الحماية نفسه الذي حققته أوروبا.

النتائج التحليلية

لقد بينت النتائج بوضوح أن الحماية الإدارية للبيانات الشخصية في كل من الإمارات ومصر شهدت خلال الأعوام الأخيرة نقلة نوعية على مستوى الإطار التشريعي والمؤسسي، غير أن هذه النقلة لم تُترجم بعد إلى منظومة مكتملة قادرة على تحقيق الامتثال الفعلي بمستوى يوازي التجارب الدولية المتقدمة. فمن جهة، وضعت الإمارات قانونًا شاملاً لعام 2021 تضمن نصوصًا متقدمة على مستوى الحقوق الفردية وآليات الإنفاذ الإداري، وهو ما يجعله أقرب إلى النموذج الأوروبي من حيث البنية. ومن جهة أخرى، سارت مصر في اتجاه مغاير حين ركّزت على إنشاء جهاز إداري مركزي —مركز حماية البيانات الشخصية— وأسندت له صلاحيات واسعة تتعلق بالترخيص والمراقبة.

هذا التباين في الفلسفة التشريعية انعكس على مستوى الفعالية. ففي الإمارات، يواجه مكتب حماية البيانات تحديات متعلقة بالاستقلالية وضعف القدرات البشرية، وهو ما يقلل من تأثير النصوص المتقدمة على أرض الواقع. أما في مصر، فإن المركز يعاني من فجوة بين حجم الصلاحيات القانونية الممنوحة له وبين إمكاناته الفعلية المحدودة، سواء على مستوى الموارد أو الكوادر الفنية المتخصصة. وهذا ما يجعل التجربة المصرية أكثر عرضة لتفاوت الامتثال بين القطاعات، خصوصًا مع نفوذ الشركات العالمية.

كما أظهرت النتائج أن الجزاءات الإدارية —رغم كونها خطوة مهمة— لا تزال محدودة الأثر مقارنة بالنظام الأوروبي. ففي حين أن الغرامات الأوروبية تصل إلى مستويات رادعة تجعل الامتثال خيارًا استراتيجيًا للشركات، تظل الغرامات العربية أقرب إلى رمزية جزئية قد لا تحقق الأثر المطلوب. هذا الوضع يجعل بعض المؤسسات تنظر إلى العقوبة على

أنها تكلفة تشغيلية يمكن تحملها بدلًا من اعتبارها تهديدًا وجوديًا. وهو ما يقود إلى الاستنتاج بأن فعالية الردع ترتبط بصرامة الجزاءات أكثر من ارتباطها بوجودها الشكلي.

إلى جانب ذلك، كشفت النتائج عن فجوة عميقة بين النصوص والتطبيق. فالتشريعات الوطنية —رغم أهميتها— ما زالت تعاني من محدودية في التطبيق العملي بسبب غياب آليات إلزامية للتقارير الدورية، وضعف الشفافية، وانخفاض مستوى الثقافة المؤسسية حول أهمية حماية البيانات. ويُلاحظ أن المبادئ الدولية للحوكمة، مثل المساءلة والشفافية، لم تُفعل بشكل كامل داخل المؤسسات، مما يترك مساحة واسعة للانتهاكات المحتملة، خاصة في بيئات إدارية غير مستقرة.

أخيرًا، أوضحت النتائج المقارنة مع التجربة الأوروبية أن ثمة فجوة هيكلية تتمثل في ضعف الاستقلالية المؤسسية، وهشاشة آليات التعاون الدولي، وضعف فعالية الرقابة الإدارية. هذه الفوارق تجعل الحماية الإدارية في الدول العربية أقرب إلى المرحلة التأسيسية التي تحتاج إلى مزيد من التطوير المؤسسي والتشريعي حتى ترقى إلى مستوى الممارسات الدولية المتقدمة.

الخلاصة العامة للنتائج

تشير النتائج الموسّعة إلى أن التشريعات الوطنية في الإمارات ومصر مثلت خطوة مهمة في اتجاه تكريس الحق في الخصوصية وحماية البيانات، لكنها ما تزال تعاني من أوجه قصور تتعلق بالشمولية، وباستقلالية الأجهزة الإدارية، وبضعف الجزاءات، وبالفجوة بين النصوص والتطبيق. كما أن انعكاس مبادئ الحوكمة الدولية كان محدودًا، ولم يُترجم إلى ممارسات مؤسسية صارمة. وتكشف المقارنة مع النموذج الأوروبي أن التجربة العربية تحتاج إلى تعزيز استقلالية الأجهزة الإدارية، وزيادة صرامة العقوبات، وتبني آليات تعاون إقليمي ودولي لمواجهة الطبيعة العابرة للحدود للبيانات الرقمية.

الاستنتاجات و التوصيات

الاستنتاجات

اولا: الإطار التشريعي لحماية البيانات الشخصية

يمكن القول إن التشريعات الوطنية في الإمارات ومصر مثلت نقلة مهمة في تكريس الحق في الخصوصية، لكنها لم تبلغ بعد مستوى الشمولية والفعالية الذي يضمن حماية متكاملة. فالقانون الإماراتي أكثر تفصيلًا وحقوقية، بينما يميل القانون المصري إلى البنية المؤسسية، وكلاهما بحاجة إلى مراجعة لتقوية الجوانب التي أهملها.

ثانيا: دور المؤسسات الإدارية في تطبيق الحماية القانونية للبيانات

أظهرت النتائج أن الأجهزة الإدارية المختصة بالحماية تلعب دورًا محوريًا، غير أن ضعف استقلاليتها ونقص كفاءاتها الفنية يمثلان عقبة رئيسية. هذه النتيجة تعكس ضرورة تعزيز البنية المؤسسية وضمان استقلالية الأجهزة بما يتوافق مع مبادئ الحوكمة.

ثالثا: الجزاءات التنظيمية بين الفعالية والضمانات في حماية البيانات الشخصية

رغم إدراج العقوبات الإدارية ضمن القوانين، إلا أن فعاليتها تبقى محدودة لضعف صرامتها مقارنة بالمعايير الدولية. وهذا يضعف من قدرة النظام القانوني على فرض الامتثال، ويجعل الحاجة ملحة إلى إصلاح تشريعي يربط العقوبات بحجم الضرر والإيرادات الفعلية للمؤسسات.

رابعا: الحوكمة كمدخل لضمان حماية البيانات الشخصية

أظهرت النتائج أن مبادئ الحوكمة الدولية انعكست في النصوص بشكل جزئي، لكنها لم تتحول إلى آليات عملية داخل المؤسسات. وهذا يبرز الفجوة بين النصوص والتطبيق، ويؤكد أن الحوكمة ليست مجرد شعارات قانونية، بل هي ممارسات مؤسسية تتطلب التزامًا طويل المدى.

خامسا: الإطار الدولي المقارن لحوكمة وحماية البيانات

أثبتت التجربة الأوروبية أنها الأكثر نضجًا من حيث الاستقلالية المؤسسية وصرامة الجزاءات وآليات التعاون الدولي، ما يجعلها نموذجًا يمكن الاسترشاد به. غير أن تبني النموذج الأوروبي بحذافيره قد لا يتناسب مع السياق العربي، وهو ما يتطلب تكييفه وفق الخصوصيات الاجتماعية والاقتصادية والإدارية للدول العربية.

التوصيات

1. **تعزيز الاستقلالية المؤسسية** عبر فصل الأجهزة الإدارية لحماية البيانات عن السلطة التنفيذية، وضمان تمويلها المستقل.
2. **رفع صرامة العقوبات** لتكون أكثر تناسبًا مع حجم الانتهاكات، مع استحداث عقوبات تصاعدية تحقق الردع.
3. **تفعيل مبادئ الشفافية** عبر إلزام المؤسسات بنشر تقارير دورية توضح كيفية جمع البيانات ومعالجتها.
4. **بناء القدرات البشرية** من خلال برامج تدريبية متخصصة لإعداد خبراء محليين في حماية البيانات.
5. **تعزيز التعاون الإقليمي والدولي** لإنشاء آليات تبادل خبرات ومعلومات بين الدول العربية لمواجهة التحديات العابرة للحدود.
6. **إطلاق حملات توعية** تستهدف القطاعين العام والخاص لتعزيز الثقافة المؤسسية والمجتمعية بأهمية حماية البيانات.

References

Abu Khumra, M. (2021). Civil protection of personal data in Arab legislation. *Journal of Legal Studies, 12*(2), 88–115.

Ibrahim, S. (2025). Administrative protection of data between national legislation and international standards. *Arab Journal of Administration and Law, 17*(1), 44–72.

Al-Bustani, A. (2025). The legal framework for privacy protection in Emirati legislation. *International Journal of Law and Administration, 8*(1), 15–40.

Al-Barwani, L. (2022). Administrative sanctions in personal data protection laws: A comparative study. *Journal of Law and Politics, 10*(3), 201–230.

Al-Qatatsha, R. (2022). Criminal protection of personal data in Arab legislation. *Journal of Contemporary Law, 9*(4), 150–178.

Hussein, M. (2020). The right to privacy and data protection in light of international conventions. *Arab Journal of Human Rights, 6*(2), 65–98.

Khalid, A. (2020). European principles of data protection (GDPR) and their potential application in the Arab world. *Journal of Legal Research, 14*(1), 33–70.

Osman, H. (2025). Administrative dimensions of legal protection of personal data. *Arab Journal of Public Policy, 11*(2), 55–84.

Al-Hinai, F. (2025). Governance of personal data between national legislation and international standards. *Journal of Sharia and Law, 19*(2), 121–156.

Mahmoud, K. (2022). The National Center for Personal Data Protection: A legal and institutional evaluation. *Journal of Administrative and Legal Studies, 15*(3), 200–235.

Ibrahim, S. (2025). *Criminal protection of electronic personal data*. Cairo: Dar Al-Fikr Al-Jami‘i.

Al-Rashed, S. (2020). Administrative protection of data between theory and practice. *Journal of Administration and Law, 11*(1), 99–128.

Wajdi, S. (2018). Legal protection of the right to informational privacy. *Journal of Communication in Humanities and Social Sciences, 24*(2), 55–77.

Al-Taie, A. (2022). Good governance in the digital domain: Towards a framework for personal data protection. *International Journal of Governance and Law, 15*(4), 200–230.

Court of Justice of the European Union (CJEU). (2016). *Judgment on privacy and data protection rights*. Luxembourg: CJEU.

European Parliament & Council. (2016). *Regulation (EU) 2016/679 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 – GDPR)*. Official Journal of the European Union, L119, 1–88.

Organization for Economic Cooperation and Development (OECD). (2013). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris: OECD Publishing.

United Nations. (2018). *Guidelines concerning Computerized Personal Data Files*. New York: United Nations Department of Economic and Social Affairs.

United Nations Human Rights Council. (2015). *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*. A/HRC/27/37. Geneva: UN.