مجلة العلوم الشاملة
المجلد (10) العدد (40)، مايو 2026
ردمد: 3014-6266
عدد خاص بالمؤتمر العلمي الدولي الأول لأبحاث التنمية المستدامة عن بعد 12-14 مايو 2026

دور الأتمتة في تعزيز استدامة الإدارة المحلية

دراسة في الأبعاد الإدارية والجنائية

د. وردة عبدالله الخنجاري
أستاذ مشارك بكلية القانون/ جامعة الزاوية
w.alkenjari@zu.edu.ly

د/ مروى محمد المودي
أستاذ مشارك بكلية القانون/ جامعة الزاوية
m.almoudi@zu.edu.ly

تاريخ الاستلام:2026/3/1 -تاريخ المراجعة: 2026/3/4- تاريخ القبول: 2026/3/9- تاريخ للنشر: 2026 /5/12

الملخص.

يسعى هذا البحث إلى بيان دور الأتمتة في تعزيز استدامة الإدارة المحلية من خلال تحليل أثر توظيف التقنيات الرقمية والأنظمة الإلكترونية في تطوير الأداء المؤسسي وتحسين كفاءة العمل الإداري، بما يسهم في تعزيز الشفافية والحوكمة الرشيدة والحد من الممارسات غير المشروعة داخل مؤسسات الإدارة المحلية. ويأتي هذا الإهتمام في ظل التحولات المتسارعة التي يشهدها العالم في مجال التحول الرقمي، وما يفرضه ذلك من ضرورة تحديث أساليب الإدارة المحلية وتطوير آليات تقديم الخدمات بما يحقق الكفاءة والفعالية والاستدامة. وتعتمد الدراسة على المنهج الوصفي التحليلي لدراسة أثر تطبيق الأتمتة في تبسيط الإجراءات الإدارية وتسريع انجاز المعاملات والحد من التعقيدات البيروقراطية المرتبطة بالإجراءات التقليدية، الأمر الذي يسهم في تحسين جودة الخدمات العامة وتعزيز كفاءة إدارة الموارد داخل وحدات الإدارة المحلية، ودعم عملية اتخاذ القرار الإداري من خلال توفير قاعدة بيانات دقيقة وأنظمة معلومات متكاملة تمكن متخذي القرار من التخطيط الفعال ومتابعة الأداء المؤسسي بصورة أكثر دقة وشفافية. وفي هذا السياق تسهم الأتمتة في تعزيز النزاهة المؤسسية من خلال توثيق الإجراءات والمعاملات إلكترونياً، بما يحد من فرص ارتكاب بعض الجرائم الإدارية والمالية مثل الرشوة والتزوير وإساءة استعمال السلطة، وذلك نتيجة تقليل الاحتكاك المباشر بين الموظف والمراجع وإتاحة إمكانية تتبع العمليات الإدارية وتعزيز آليات المراقبة والمساءلة. كما يتطرق البحث إلى التحديات القانونية والتنظيمية المرتبطة بتطبيق الأتمتة، لا سيما ما يتعلق بحماية البيانات وضمان أمن المعلومات داخل المؤسسات المحلية.

ويلخص البحث إلى أن الأتمتة تمثل أحد المرتكزات المهمة لتحقيق استدامة الإدارة المحلية تعزيز كفاءتها، شريطة توفير بنية تحتية تقنية مناسبة، وتأهيل الكوادر البشرية، وتطوير الأطر التشريعية التي تنظم استخدام التقنيات الرقمية بما يضمن تحقيق الشفافية والكفاءة في العمل الإداري.

الكلمات المفتاحية: الأتمتة، الإدارة المحلية، الاستدامة الإدارية، التحول الرقمي، الجرائم المعلوماتية.

Abstract.

This research aims to demonstrate the role of automation in enhancing the sustainability of local administration by analyzing the impact of employing digital technologies and electronic

systems on developing institutional performance and improving the efficiency of administrative work. This contributes to strengthening transparency and good governance, and reducing illicit practices within local government institutions. This focus arises from the rapid transformations the world is witnessing in the field of digitalization, and the resulting need to modernize local administration methods and develop service delivery mechanisms to achieve efficiency, effectiveness, and sustainability. The study employs a descriptive-analytical approach to examine the impact of implementing automation on simplifying administrative procedures, expediting transactions, and reducing bureaucratic complexities associated with traditional procedures. This contributes to improving the quality of public services, enhancing the efficiency of resource management within local government units, and supporting administrative decision-making by providing an accurate database and integrated information systems that enable decision-makers to plan effectively and monitor institutional performance more accurately and transparently. In this context, automation contributes to enhancing institutional integrity by electronically documenting procedures and transactions, thereby reducing opportunities for certain administrative and financial crimes such as bribery, forgery, and abuse of power. This is achieved by minimizing direct contact between employees and clients, enabling the tracking of administrative processes, and strengthening oversight and accountability mechanisms. The research also addresses the legal and regulatory challenges associated with implementing automation, particularly those related to data protection and information security within local institutions.

The research concludes that automation is a key pillar for achieving sustainable and efficient local governance, provided that a suitable technological infrastructure is in place, human resources are trained, and legislative frameworks are developed to regulate the use of digital technologies, ensuring transparency and efficiency in administrative work.

Keywords: Automation, Local Government, Administrative Sustainability, Digital Transformation, Cybercrime.

المقدمة.

يعد التحول الرقمي أحد أهم العوامل المسؤولة عن النمو الاقتصادي والتنمية المستدامة، والذي بات ضرورة ملحة في ظل التحديات والفرص التي تواجه العالم في القرن الحادي والعشرين، وقد شمل جميع المجالات والقطاعات، بما في ذلك الجهاز الإداري للدولة، الذي يعد العمود الفقري للحكم الرشيد والتنمية المستدامة.

ويعد مفهوم الأتمتة مفهوماً حديثاً ظهر نتيجة للتقدم التقني، نتج عن ثورة تكنولوجيا المعلومات أثاراً كبيرة في تطوير العمليات الإدارية في كافة جوانبها الإدارية والقانونية، حيث أصبحت تكنولوجيا الاتصالات وتقنية المعلومات أساساً هاماً في منظومة تسير أعمال الإدارات، وداعماً لتحقيق أهدافها وتبسيط العمليات الإدارية وتحسين كفاءتها وخدمة رشاقة هياكلها التنظيمية من خلال التحول الرقمي، والسعي لتحقيق متطلبات الاستدامة المؤسسية وتعزيز القدرة على استخدام تكنولوجيا المعلومات والاتصالات بشكل فعال.

وتعد أتمتة القرارات الإدارية من أبرز تطبيقات تكنولوجيا المعلومات في الإدارة بهدف توظيف التطبيقات التكنولوجية كتقنيات الذكاء الاصطناعي، والتعلم الآلي، وأدوات تحليل البيانات الحديثة لدعم صناعة القرارات ووضع بدائل مناسبة، وتمكين الإدارة من اتخاذ القرارات بشكل ذكي وفعال، وهو ما تعززه الأتمتة كأداة قوية لتحسين جودة وفاعلية وكفاءة القرارات الإدارية وضبط إطارها القانوني وتعزيز اتساقها وموضعيتها، وتحقيق التكامل بين الأنظمة المختلفة.

فالأتمتة الإدارية عموماً وأتمتة القرارات الإدارية خصوصاً تعتبر نقلة نوعية في مجال القانون الإداري، ولذا تحتاج إلى وضع وسائل فعالة لضمان توافقها مع المتطلبات القانونية في صناعة القرارات الإدارية. إضافة إلى ذلك تتضمن عمليات التحول الرقمي مخاطر متعددة تتعلق بطبيعة الأتمتة، والتحول الرقمي ومخاطره ذات الطبيعة الخاصة، والتي ترتبط بتطبيقها، فيجب أن يتم الإعداد الجيد لبيئة قانونية ملائمة وآمنة، وداعمة لتطبيق التقنيات الحديثة في مجال الإدارة العامة.

إن التنمية المستدامة هي الركيزة الأساسية للمجتمع وتطوره من خلال بحثها عن اقتصاد قوي لتحسين المستوى المعيشي، ولتحقيق نوعية الحياة الأمثل للإنسان، فإن جوهرها هو تلبية الحاجيات وتوفير الحياة الكريمة مع التفكير في المستقبل ومصير الأجيال القادمة لتحقيق كافة متطلباتهم.

وتعد الإدارة المحلية توزيع للمهام الإدارية بين الحكومة المركزية وبين الهيئات المحلية المنتخبة كما تعد الحلقة الوسيطة بين الحكومة المركزية والمواطن المحلي ولذلك فهي تتولى مهاماً تحت إشراف الحكومة ورقابتها للإدارة المحلية ويظهر ذلك من خلال توسيع فرص المشاركة في وضع الخطط والكشف عن مستحقات المجتمع المحلي لتنظيم حياة الأشخاص وممارسة الحكم الصالح، وفي هذه الحالة تأخذ شكل العلاقة الدائرية التفاعلية بين الإدارة المحلية والتنمية المستدامة على أساس أن مصطلح التنمية المستدامة أصبح محل اهتمام و أحد الأفكار من الأفكار التي تربط بين البيئة والتنمية الاقتصادية والاجتماعية ومتطلباتها.

ولا يزال العالم اليوم يواجه تحديات كبيرة في مجالات التنمية خاصة ما يتعلق بأبعادها الثلاثة الاقتصادية والاجتماعية والبيئية، وتواجه الإدارة المحلية تحديات متزايدة تتعلق بتحسين جودة الخدمات وترشيد الموارد والاستجابة لمتطلبات التنمية المستدامة.

وتشهد الإدارة العامة تحولاً رقمياً متسارعاً نتيجة التطور التكنولوجي والاعتماد المتزايد على أنظمة الأتمتة والذكاء الاصطناعي. وقد برزت الأتمتة كأداة استراتيجية لتحسين أداء وحدات الإدارة المحلية من حيث الكفاءة والشفافية، وسرعة الإنجاز، وضبط الإجراءات. غير أن هذا التحول يثير إشكالات قانونية وجنائية تتعلق بحماية البيانات، والمسؤولية عن الأخطاء التقنية، والجرائم المعلوماتية.

لذلك يقتضي تحقيق التنمية المستدامة إجراءات وسياسات عالمية ووطنية يكون من شأنها التقليل من هذه الفجوة، وإحراز مزيد من التقدم في المجالات التنموية الرئيسية (الاقتصادية، الاجتماعية، والبيئة،) مما يتطلب تحقيق النمو وتوفير فرص العمل، مع القيام في الوقت ذاته بتعزيز الاستدامة.

ومع التطور التكنولوجي، أصبحت الأتمتة والتحول الرقمي من أهم الأدوات التي تسهم في رفع كفاءة الأداء الإداري وتعزيز الاستدامة بأبعادها المختلفة.

أهمية البحث.

تنبع أهمية الدراسة من الحاجة إلى تحليل أثر الأتمتة في تطوير الإدارة المحلية، مع الوقوف على التحديات القانونية والجنائية المصاحبة لها.

وتتمثل الأهمية العلمية في:

- إثراء الدراسات القانونية والإدارية المتعلقة بالتحول الرقمي.
- تحليل العلاقة بين التكنولوجيا والمسؤولية الجنائية.

أما الأهمية العملية فتتمثل في:

- دعم صناع القرار في تطوير سياسات الأتمتة.
- تقديم توصيات لتعزيز الحوكمة الرقمية والحد من المخاطر الجنائية.

أهداف البحث.

يسعى هذا البحث إلى تحقيق مجموعة من الأهداف العلمية والعملية، يمكن إجمالها فيما يلي:

1- بيان مفهوم الأتمتة وأسسها في الإدارة المحلية.

2- تحليل الأبعاد الإدارية للأتمتة وأثرها في الكفاءة والشفافية.

3- تحليل دور الأتمتة في تعزيز استدامة الإدارة المحلية، وبيان أثارها الإيجابية والمخاطر الجنائية المرتبطة بها، وصولاً إلى صياغة تصور قانوني يحقق التوازن بين متطلبات التحول الرقمي وضمان الحماية الجنائية.

4- دراسة الأبعاد الجنائية المرتبطة بالتحول الرقمي.

5- اقتراح آليات قانونية وتنظيمية لضبط العمل الإداري المؤتمت.

إشكالية البحث.

في ظل التوجه العالمي نحو التحول الرقمي واعتماد الأتمتة في تسيير المرافق العامة، أصبحت الإدارة المحلية أمام تحول جوهري في بنيتها التنظيمية وآليات عملها، بما ينسجم مع توجهات الأمم المتحدة لتحقيق أهداف التنمية المستدامة غير أن هذا التحول، رغم ما يحمله من مزايا تتعلق بالكفاءة والشفافية وترشيد الموارد، يثير في المقابل إشكالات قانونية وجنائية ترتبط بأمن المعلومات، وحماية البيانات وتحديد المسؤولية الجنائية عن الجرائم المرتبطة للأنظمة المؤتمتة.

ومن ثم تتمحور إشكالية البحث في السؤال التالي:

إلى أي مدى تسهم الأتمتة في تعزيز استدامة الإدارة المحلية وكيف تؤثر في الأبعاد الإدارية والتنظيمية، وما حدود المخاطر الجنائية المترتبة على استخدامها، وكيف يمكن تحقيق التوازن بين متطلبات التطور الرقمي وضمان الحماية الجنائية الفعالة؟

فرضيات البحث.

ينطلق البحث من مجموعة من الفرضيات العلمية القابلة للتحليل تتمثل فيما يأتي:

- يسهم اعتماد الأنظمة المؤتمتة في تقليل مظاهر الفساد الإداري التقليدي، لكنه في المقابل يفرز أنماطاً جديدة من الجرائم ذات الطابع الإلكتروني.
- يؤدي التحول الرقمي إلى ظهور أنماط جديدة من الجرائم المعلوماتية.
- الإطار التشريعي الجنائي التقليدي غير كافٍ لمواجهة الجرائم المرتبطة بالأتمتة، ما لم يتم تطويره ليتلاءم مع الطبيعة التقنية لهذه الجرائم.
- تعزيز الأمن السيبراني والرقابة الرقمية الداخلية في وحدات الإدارة المحلية يؤدي إلى تقليص المخاطر الجنائية المرتبطة بالأتمتة دون إعاقة مسار التحول الرقمي.

منهجية البحث.

من أجل الوقوف على دور الأتمتة في تعزيز استدامة الإدارة المحلية، والوصول إلى النتائج المرجوة، تم الاعتماد على المنهج الوصفي والتحليلي، وذلك من خلال وصف وبيان المفاهيم المرتبطة بموضوع الدراسة، وتحليل النصوص القانونية ذات الصلة.

خطة البحث.

من أجل تحقيق أهداف البحث والإجابة عن الإشكالية المطروحة فقد تم تقسيم البحث إلى مبحثين، تضمن المبحث الأول دراسة الأتمتة كآلية لتعزيز استدامة الإدارة المحلية، أما المبحث الثاني فتم تخصيصه لدراسة الحماية التقنية والجنائية للإدارة المحلية المؤتمتة كضمانة لاستدامتها.

المبحث الأول: الأتمتة كآلية لتعزيز استدامة الإدارة المحلية.

في ظل اتجاه الدولة بكافة جهاتها ومؤسساتها نحو التحول الرقمي باعتباره مشروعا قوميا في سبيل الوصول

لمرحلة الحكومة الرقمية، تظهر لدينا تحديات قانونية قد تقف عائقا في طريق تحقيق هذه المرحلة، ولعل أهم ظاهرة في مشروع التحول الرقمي هو **"أتمتة الإجراءات الإدارية"** وتعتبر الأتمتة الإدارية – في صورتها البسيطة– هي تسيير الإجراءات الإدارية بشكل آلي وبأقصى دقة ممكنة وبأقل أخطاء محتملة وذلك بفضل استخدام أنظمة تكنولوجيا المعلومات الحديثة وتقنيات الذكاء الاصطناعي وهي بتلك الصفة تعد سمة إيجابية من سمات العصر الرقمي الحالي الذي نعيش به، بيد أنها لا تخلو من المثالب حيث إن التساؤل الأساسي الذي يدور في الذهن هو ما أثر هذه الإجراءات الإدارية التي هي في حقيقتها حزمة من القرارات الإدارية أمام مبدأي المشروعية والملائمة هل من شأن الاتجاه إلى الأتمتة الإدارية في حالات وجود سلطة تقديرية لجهة الإدارة، وكيف سيتم معالجة ذلك الأمر.

كما يثور تساؤل أيضا عن التحديات القانونية التي ستواجه تطبيق الأتمتة على القرارات الإدارية والتي تأتي اعتبارات الملائمة أكبر عائق أمام تطبيق الأتمتة فإذا ما حدث خطأ بهذه الأنظمة أحدثت خللا بالمراكز القانونية للأفراد، فما هو الحكم آنذاك.

ومن ثم سنتعرض لبحث تعزيز الاصلاح المؤسسي وتطوير العمليات الادارية باستخدام الأتمتة في "المطلب الأول"، ثم نستعرض الإشكاليات القانونية التي تواجه الأتمتة الإدارية في " المطلب الثاني".

المطلب الأول: تعزيز الاصلاح المؤسسي وتطوير العمليات الإدارية باستخدام الأتمتة.

تشهد موضوعات القانون الإداري ككل تحولاً هاماً في ضوء التقدم التكنولوجي وتبني الحكومات للإدارة الإلكترونية وأتمتة العمل الإداري [(1)].

ويعد هذا التحول تطويراً للقانون الإداري التقليدي، مما يفتح أبواباً أمام توجهات جديدة ومستقبلية في تنظيم صدور القرارات المؤتمتة، فتكييف المفاهيم القانونية التقليدية المتعلقة بالقرارات الإدارية بما يتوافق مع التحول التكنولوجي، وتوظيف التقنيات الحديثة في صنع القرارات [(2)]. وتحقيق التوازن بين المرونة وخدمة الصالح العام، والأهداف الأساسية للقرارات الإدارية والتطور التكنولوجي [(3)]، وضمان حماية الأسس القانونية والواقعية للقرارات الإدارية.

---

[1] – محمد البداوي، القرار الإداري الإلكتروني، مجلة المنارة للدراسات القانونية والإدارية، 2018، العدد 23، ص21.

[2] – أحمد بن محمد الهرماس الشمري، أثر وسائل الاتصال الإلكترونية في نفاذ القرارات الإدارية، مجلة البحوث القانونية والاقتصادية، 2020، ص42.

[3] – علاء محي الدين مصطفى أبو أحمد، القرار الإداري الإلكتروني، مجلة البحوث القانونية والاقتصادية، 2015، العدد 25 (42)، ص429.

وتعد الأتمتة [4] والتحول الرقمي في العمليات الإدارية ما هو إلا نتيجة للتقدم التكنولوجي، وشكل من أشكال مساهمة مخرجات الثورة التقنية في تحسين العمليات الإدارية، من خلال توظيف تقنيات المعلومات والاتصالات في ابتكار تقنيات حديثة لإنجاز المهام وتوفير البدائل والحلول المتطورة.

فمع التقدم التكنولوجي الهائل الذي يشهده العالم في الوقت الحاضر، لا يمكن تجاهل تأثير الأتمتة على كافة جوانب الحياة، بما في ذلك مجال الإدارة المحلية [5].

فتعني أتمتة العمليات الإدارية استخدام التقنيات الحديثة بشكل يومي ومستمر في تنفيذ العمليات الإدارية، بهدف زيادة إنتاجية وفاعلية الأعمال في الهيئات والمؤسسات من خلال الاستفادة الشاملة من تقنيات المعلمات"[6].

ويعرف (O'Brien) الأتمتة الإدارية بأنها: "الاعتماد على أجهزة الحاسب وتطبيقاته بفرض تنظيم الأعمال الإدارية، والتقليل من العمل اليدوي؛ لتحقيق السرعة والدقة في الأداء"[7].

وتعتمد الأتمتة الإدارية على استخدام أدوات وأنظمة الكترونية حديثة بهدف تنظيم وتنفيذ الأعمال الإدارية التي يقوم بها الموظفون وتحقق السرعة والدقة في الأداء والإنتاج، وتعزيز قدرة العاملين على تنفيذ المهام بكفاءة عالية [8].

وتتضمن تقنيات الأتمتة الإدارية مجموعة من أنظمة الموارد البشرية، وأنظمة الإدارة الإلكترونية، وغيرها مما يسهم في تبسيط وتنظيم العمليات الإدارية، وتحسين توصيل المعلومات، والتعاون بين الأفراد والإدارات المختلفة.

---

[4] – الأتمتة هو مصلح معرب من الإنجليزية (Automation) ويعني التشغيل الآلي أو الذاتي، ويطلق على العمليات التي تعمل ذاتيا بدون تدخل بشري باستخدام أجهزة الحاسب الآلي المبنية على المعالجات والبرمجيات. فهي فن جعل الإجراءات تنفذ بشكل تلقائي، ولقد شاع استخدام هذا المصطلح رغم ما اكتنفه من غموض وإشكاليات لغوية بين الباحثين العرب. فنجد أن بعضهم استخدم لفظ الآلية أو الأتوماتكية، والميكنة، والمكننة، أنظر: حسن عواد السريحي، وآخرون: أتمتة أعمال المكاتب (دراسة تطبيقية على إمارة مكة المكرمة)، دار المريخ للنشر والتوزيع، الرياض، المملكة العربية السعودية، 1999م، ص11.

[5] – تعرف الإدارة المحلية على أنها: "أسلوب الإدارة بمقتضاها يقسم إقليم الدولة إلى وحدات ذات مفهوم محلي، تتمتع بشخصية اعتبارية ويمثلها مجالس منتخبة من أبنائها لإدارة مصالحها تحت اشراف ورقابة الحكومة المركزية. انظر: خالد سمارة الزعبي، تشكيل المجالس المحلية، مكتبة دار الثقافة، عمان، ط3، 1993، ص119.

[6] – عثمان يوسف محمد العبيد، دور الأتمتة الرقمية في البلدية للدوائر الإدارية، المالية والفنية، مجلة رماح للبحوث والدراسات، 2022، العدد٦٦، ص 4.

[7] – بخيث مبارك الراشدي، أثر الأتمتة على تحسين قيادة المؤسسات، مجلة المعرفة، المغرب، العدد الثلاثون، 2025، ص184.

[8] – دعاء محمد إبراهيم، الأتمتة ودورها في دعم صناعة القرار الإداري من الناحية الإدارية والقانونية، مجلة الكوفة للعلوم القانونية والسياسية، جامعة الكوفة، كلية القانون، العراق، المجلد 17، العدد 59، 2024، ص67.

الفرع الأول: أبعاد الأتمتة الإدارية وأثارها.

يمكن التعرف على الأبعاد الإدارية من جانبين الأول يتعلق بالعمليات والأنشطة داخل التنظيم والجانب الثاني يتعلق بهيكل التنظيم وعناصره المختلفة.

أولاً: مدى تأثير الأتمتة على العمليات التنظيمية.

تؤدي الأتمتة إلى تحقيق درجة أعلي من التكامل والترابط بين الأنشطة التنظيمية المختلفة باعتبارها نظماً فرعية تعمل جميعاً في إطار نظام أكبر كالربط بين نظامي المستودعات والمشتريات والذي ينعكس على مدى التغيير الذي يشمل وظيفة التخطيط الإداري ووظيفة الرقابة والمتابعة من جانب ومن جانب آخر التغيير في خصائص ومهارات المديرين[9].

كما يخلق توظيف الأتمتة تغييرات هامة في مجال الأنشطة المكتبية والكتابية وتدفق العمليات الروتينية ونوعيات النماذج وتصاميمها والسجلات المستخدمة في التنظيم وهذا الجانب يعكس بوضوح التأثير الملموس للأتمتة في التنظيم الاداري حيث أن هذه الأنشطة تتسم عادة بضخامة حجمها وانتشارها في كل أركان التنظيم ومن ثم ضخامة عدد الأفراد العاملين بها والوقت المستغرق فيها كعمليات إصدار القرارات وإمساك الدفاتر وحسابات المستودعات والرقابة عليها وحسابات الأجور والمرتبات وغيرها [10].

كما يترتب على توظيف الأتمتة في الأنشطة الإدارية آثار بارزة على التنظيم أهمها:

1. تخفيض عدد العاملين في الأنشطة التي توظف فيها الأتمتة.
2. تغيير في نوعيات المهارات اللازمة للعاملين.
3. إمكانية مركزية العمليات وإحكام السيطرة عليها.
4. يؤدي الاعتماد على الأتمتة في عمليات الأنشطة الإدارية وضبط الجودة وغيرها من الأنشطة الحيوية في التنظيم إلى زيادة الاتجاه نحو إنشاء نظم متكاملة للمعلومات تعتمد على بنوك المعلومات وترشيد عمليات اتخاذ القرارات وإمكانية تطبيق أساليب متطورة لحل المشكلات كبحوث العمليات، والمحاكاة، ونظرية المباريات[11].

---

9 – ناصر بن منيف العتيبي، الأتمتة ودورها في تحسين أداء إدارات الموارد البشرية في الأجهزة الأمنية بمدينة الرياض، رسالة دكتوراه، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الإدارية الرياض، 2007، ص94.

10 – محمد نور برهان، الموارد البشرية في الفنادق، دار الصفاء للنشر والتوزيع، عمان، 1998، ص126.

11 – علاء عبد الرازق السالمي، محمد عبدالعال النعيمي، أتمتة المكاتب، الطبعة الأولى، دار المناهج للنشر والتوزيع، الرياض، 1999، ص318-320.

ثانياً: أثر الأتمتة على العمليات الإدارية.

تنعكس آثار توظيف الأتمتة على وظيفة التخطيط ومن أبرز ملامح التغيير في هذا الجانب ما يلي [12].

أ. ساعدت على توفير قدر أكبر من المعلومات الدقيقة عن كافة مجالات العمل مما ساعد الإدارة على وضع خطط سليمة واستراتيجية فعالة.

ب. بات ممكناً إعداد خطط تأخذ في اعتبارها التفاعل بين عدد أكبر من المتغيرات مما يساعد على تقويم آثار هذه المتغيرات على نتائج الخطط وفق أسس علمية موضوعية بعد أن كان يعتمد على تقديرات وأحكام شخصية.

ج. بات ممكنا اختبار النتائج المحتملة لعدد من القرارات البديلة وبالتالي فأسلوب التجربة والخطأ في اتخاذ القرارات قد انتقل من التجربة في الواقع (المفترضة) إلى التجربة الفعلية مما وفر الجهد والوقت وتجنب الخسارة وتعظيم العائد.

د. يمكن إتباع نظم التخطيط المرن بفضل طاقات النظم الآلية الضخمة فيمكن تعديل الخطط بسرعة استجابة للتغيرات في الظروف والأوضاع المختلفة.

هـ. أصبح ممكنا تحقيق التخطيط الشامل الذي ينظر إلى التنظيم باعتباره نظاما متكاملا.

كما تعكس الأتمتة أبعاداً ايجابية في مجال الرقابة الإدارية من خلال القدرة على وضع معايير رقابية وإعداد نظم للرقابة الشاملة وتخفيض الفارق الزمني بين التنفيذ والرقابة وإعداد تقارير رقابية شاملة وسريعة والى التوسع في نتائج الرقابة .

الفرع الثاني: أتمتة المعاملات الإدارية في الإدارة المحلية بين متطلبات التحول الرقمي ومعوقات التطبيق.

يكشف واقع أتمتة العمليات والأنشطة الإدارية في الإدارات المحلية عن تفاوت كبير في تطبيقها والذي يعكس مشكلات تتمثل في تدني مستوى الاستفادة من التقنية الحديثة المتاحة لاسيما في مجال العمليات الإدارية واقتصار الاستفادة منها على المستويات التنفيذية وباستعراض المكونات أو العناصر الأساسية للأتمتة ممثلا بالأجهزة والمعدات والأنظمة البرمجية والموارد البشرية والتطبيقات يتضح ما يلي:

أولاً: الأجهزة والمعدات.

يرى البعض وجود تفاوت كبير في عدد الحاسبات الإلكترونية من حيث الكم أو النوع في ضوء الإمكانات المادية المتاحة حيث يعاني سوق هذه الأجهزة من تنوع شديد في الأجهزة المطروحة ومنافسة

[12] – ناصر بن منيف العتيبي، الأتمتة ودورها في تحسين أداء إدارات الموارد البشرية في الأجهزة الأمنية بمدينة الرياض، مرجع سابق، ص95.

كبيرة للشركات الموردة أو بسبب مستوى التطور الاقتصادي والاجتماعي ونمط التخطيط السائد وحجم السوق وعوامل أخرى[13].

والملاحظ أنه مع وفرة الأجهزة والمعدات التقنية في الأجهزة الحكومية فإنها لا تزال غير قادرة على الوصول على مستوى الاستخدام الفعال وتوظيفها بكفاءة في الأعمال الإدارية مما يعكس وجود صعوبات تحد من فعالية توظيف الأتمتة.

ثانياً: الموارد البشرية.

تفتقر معظم الأجهزة الحكومية ولا سيما الإدارات المحلية إلى الكوادر الفنية المتخصصة في هذا المجال حيث تعاني هذه الأجهزة من نقص وندرة الكوادر المؤهلة لاستخدام النظم الحديثة فهناك فجوة بين العرض من القوى البشرية التي تنتجها المؤسسات التعليمية والتدريبية والطلب عليها من قبل الادارات المحلية بالأجهزة الحكومية ومما ضاعف من مشكلات توفير الكوادر البشرية ضعف الحوافز المادية والمعنوية المقدمة لها[14].

كما تنشأ في بعض المؤسسات العامة فجوة بين القيادات وبين التقنيين العاملين في مجال استخدام تقنية المعلومات المعتمدة على النظم الحاسوبية مما يعيق الاتصال بين الطبقتين وينتهي إلى تصميم أنظمة لا تتناسب مع الاحتياجات الفعلية لهذه القيادات ومن ثم عزوفها عن استخدام الأنظمة المؤتمة ويتطلب إعادة تصميمها وتطويرها مما يستهلك وقتا وجهدا كبيرين ويضاعف التكلفة المالية ولعل هذا سبب ضعف الكثير من المؤسسات الحكومية ومنها الإدارات المحلية عن استيعاب التقنية وتوظيفها بشكل صحيح.

ثالثاً: عدم تبني أساليب التخطيط العلمي.

تفتقر كثير من الأجهزة العامة وخصوصاً الإدارات المحلية إلى التخطيط المبني على أسس علمية لاستخدام التقنية واستثمارها استثمار أمثل على كافة المستويات الإدارية المركزية واللامركزية، وتختلف صور ونماذج التخطيط في هذا المجال والذي غالباً ما يتسم بالشكلية فدراسات الجدوى مثلاً يتم إعدادها أحيانا لضرورة الحصول على الموافقات اللازمة من الجهات العليا وليس لمعرفة الجدوى الحقيقية للمشروع.

ومن المؤكد أن أهمية التخطيط لتقنية المعلومات تتمثل في ضرورة الإعداد والتحضير لتهيئة وإيجاد البيئة المناسبة وتأمين مستلزمات الاستخدام الأمثل لتقنية المعلوماتية حيث تؤكد الدراسات والبحوث على أهمية وضع خطط طويلة الأمد للتعامل مع المتغيرات التقنية المستقبلية.

---

[13]– محمد حمدي الطعامنة، طارق العلوش، الحكومة الالكترونية في الدول العربية، المنظمة العربية للتنمية الإدارية، القاهرة، 2004، ص94.

[14]– عبدالله حسن العبد القادر، توطين تقنية المعلومات في دول مجلس التعاون الخليجي نحو إدارة مثلى، رسالة ماجستير، غير منشورة، جامعة الملك فهد للبترول والمعادن، الرياض، 2000، ص167–175.

رابعاً: عدم وجود استراتيجية تقنية.

في ظل غياب استراتيجية تقنية ينعدم التنسيق وتشتت الجهود المبذولة لاستثمار التقنية بنظمها الآلية وبرمجياتها المختلفة كما ينعدم تصور وضع الأولويات على مستوى الوحدات الإدارية المحلية أو المستوى الكلي للأجهزة العامة[15].

خامساً: الأنظمة البرمجية.

يتم الحصول على الأنظمة البرمجية اللازمة لتشغيل نظم الحاسب بشكل أساسي من الشركات الصانعة أو الموردة للأجهزة مما أدى إلى تنوع هذه الأنظمة البرمجية وتفاوت مستواها داخل الأجهزة الحكومية بالإضافة إلى عدم وجود شركات متخصصة في صناعة هذه البرامج التنظيمية في ليبيا وباقي الوطن العربي.

وفيما يتعلق ببرامج التطبيقات فمصدرها يكون في بعض الحالات داخليا من خلال الإعداد الذاتي لهذه البرامج من قبل الجهات المستفيدة وأحيانا يستعان بجهات خارجية كالشركات الموردة أو المكاتب الاستشارية المتخصصة والحصول علي هذه الأنظمة البرمجية أمر صعب التحقيق لأن ذلك يتطلب توفر كوادر فنية مؤهلة في مجال تحليل وتصميم الأنظمة وبرمجتها ويعتمد علي مدي تقدم خطط التعليم والتأهيل في هذا المجال [16].

سادساً: تطبيقات الحسابات الالكترونية.

تتباين تطبيقات الحسابات الالكترونية من حيث الشمولية ودرجة التعقيد بين الأجهزة الحكومية ومنها الادارات المحلية تباينا كبير ويرتبط مستوى التطبيق الفعلي لكل جهاز بعوامل من أهمها مستوى التطور الاقتصادي والاجتماعي وتتمثل الشمولية في تطبيقات مالية وتجارية وعلمية وتقنية وببليوغرافية والتحكم في العمليات وغيرها من التطبيقات الوظيفية المتنوعة ومن حيث درجة التعقيد تعتبر التطبيقات القائمة أنظمة آلية للأتمتة عمليات معالجة البيانات أو عمليات تسيير الإجراءات[17].

ويظل الارتقاء بهذه التطبيقات لمستوى الإدارة العليا ومساندتها في عملية اتخاذ القرارات لايزال أمراً نادراً مما يشكل عائق توظيف الأتمتة بفعالية في كافة المستويات الإدارية لبناء أنظمة معلومات إدارية متكاملة.

15 – محمد نور برهان، الموارد البشرية في الفنادق، مرجع سابق، ص192.

16 – ناصر بن منيف العتيبي، الأتمتة ودورها في تحسين أداء إدارات الموارد البشرية في الأجهزة الأمنية بمدينة الرياض، مرجع سابق، ص109.

17 – سعد غالب ياسين، الإدارة الإلكترونية وأفاق تطبيقاتها العربية، مركز الإدارة العام، المملكة العربية السعودية، 2005، ص84.

المطلب الثاني: الحوكمة التشريعية ودورها في تعزيز أتمتة نظم دعم القرار الاداري.

يقتضي اعتماد الأتمتة في الإدارة المحلية إطاراً قانونياً يوازن بين متطلبات التطور الإداري وحماية الحقوق، ويضمن الشفافية والمساءلة والخضوع لمبدأ المشروعية، تجنباً لما قد ينجم عن الاستخدام غير المشروع من مساس بالخصوصية أو الانحياز في القرارات.

وتعرف تكنولوجيا دعم القرار على أنها: "عبارة عن نظم وتطبيقات للمعلوماتية تستند إلى تقنيات عالية ومتطورة وهي عوامل ظهرت لمساندة وتعزيز القدرة على اتخاذ القرارات من قبل المديرين القائمين على المنظمات الإدارية، وتعرف نظم دعم أو مساندة القرار بأنها نظم تفاعلية حوسبة تساعد صانع القرار على استخدام البيانات والنماذج لحل المشكلات غير الهيكلية"[18]

ويشترط لتوظيف التقنيات الحديثة في العمليات الإدارية ككل وفي بناء عناصر صنع القرار الإداري وتكوين مراحله، ألا تتجاوز القواعد القانونية المعمول بها، أو تخالف مبدأ استقرار المراكز القانونية.

حيث تظهر القرارات الإدارية المؤتمتة تحديات قانونية، فيجب وضع ضوابط وأطر قانونية لتنظيم استخدامها، بما في ذلك ما يضمن شفافيتها، وعملية المساءلة، وحماية البيانات الشخصية، وتجنب التحيز والتميز.

الفرع الأول: القرار الإداري المؤتمت وضوابطه.

لقد اكتسب موضوع القرار الإداري المؤتمت أهمية كبيرة في الآونة الأخيرة نظرا لتطلع الجهات الإدارية الى تحديث وظائفها وتطويرها وفق المستجدات الراهنة والتكنولوجيا المتطورة، لما تتمتع به من صفات ومميزات تعمل على المحافظة على مرونة سير المرافق العامة بانتظام واطراد، فالأتمتة الإدارية تعني تبسيط المهام الإدارية المتكررة باستخدام الذكاء الاصطناعي وتقليل الجهد والوقت المستغرق في انجاز المعاملات المؤتمتة وهي بطبيعة الحال مرحلة من مراحل الوصول إلى التحول الرقمي، وهو مصطلح مستحدث يطلق على كل شيء يعمل آلياً دون التدخل البشري، ويتم بين العمليات ذاتياً، من خلال الاعتماد على برمجيات وخوارزميات في تقديم الخدمات بدون تدخل البشر [19].

لذلك سنبين مفهوم القرار الاداري المؤتمت ثم نتطرق إلى ضوابط اتخاذ القرارات الإدارية المؤتمتة على النحو الاتي:

---

18 – سعد غالب ياسين، نظم مساندة القرار، دار المناهج، عمان، 2006، ص21.

19 – USAID, DESIGNING AND IMPLEMENTING COURT AUTOMATION PROJECTS Practical Guidance for USAID DRG Officers August 2019, accessible on: https://www.usaid.gov/sites/default/files/2022-05/USAID-CAP-Guide FINAL.pdf تاريخ الدخول 2026/2/24.

أولاً: مفهوم القرار الإداري المؤتمت.

يعرف القرار الإداري المؤتمت على أنه: "قرار يتم اتخاذه بواسطة نظام مؤتمت يستند إلى تقنيات متعددة منها تطبيقات الذكاء الاصطناعي وأنظمة التعلم الآلي، ويستخدم هذا النوع من القرارات في العديد من المجالات الإدارية مثل الضمان الاجتماعي، ومنح التأشيرات، وإصدار التراخيص، وتقديم المساعدة الحكومية، والتحقيقات الجنائية، وغيرها. وتواجه عملية صنع القرارات الإدارية المؤتمتة تحديات تتعلق بأحكام القانون والخطوات المعتادة في صناعة القرارات الإدارية، حيث يتطلب الأمر وجود حلول لمشكلات المسؤولية والمساءلة عن القرارات المؤتمتة، واحترام سيادة القانون، وذلك بالتكيف مع هذا النوع الجديد من صنع القرارات [20].

ويتضح من هذا التعريف أن القرار الآلي هو قرار يُتخذ بشكل ذاتي من خلال منظومات ذكية تعتمد على معالجة وتحليل البيانات والمعلومات المتوفرة، حيث تقوم الخوارزميات بتوليد النتائج أو التوصيات استنادًا إلى قواعد بيانات ضخمة، تُستخدم كمرتكز لاتخاذ القرار الإداري دون تدخل العنصر البشري في عملية صنع القرار.

والهدف الأساسي من وجود الأتمتة إخراج العنصر البشري من تقديم الخدمات، أي فصل مقدمي الخدمات عن المستخدمين، وذلك عرضة درء الفساد.

ومما تقدم، يمكن أن نصل بالقول إلى أن القرار الإداري المؤتمت هو (القرار الذي يصدر من الإدارة بأسلوب مبرمج عبر الوسائل الإلكترونية بهدف تحقيق مصلحة عامة وفقاً للقوانين والأنظمة المعتمدة دون تدخل العنصر البشري).

ولتنفيذ هذه الآلية لابد من توافر ضوابط تتيح للمرفق العام العلم بمعطيات عمل الخوارزميات التي تتولى إصدار قرارات تخصه.

ثانياً: ضوابط اتخاذ القرارات الإدارية المؤتمتة.

في الواقع، أحدثت القرارات الإدارية الآلية تحوّلا كبيراً في مفهوم القرار الإداري ذاته. فقد أصبح القرار الإداري لا يعبر فقط عن إرادة الإدارة، بل أيضا عن مخرجات نظام الذكاء الاصطناعي، ولنجاح أتمتة الأعمال الإدارية وصناعة القرارات المؤتمتة ضمن إطار قانوني تقني، فينبغي تطوير القوانين واللوائح وجعلها أكثر مرونة لمواكبة التقدم التقني المتطور بشكل مستمر، فيجب أن توفر السلطة التشريعية أطر قانونية ملائمة ومبتكرة تحدد ضوابط وقواعد استخدام التقنيات المتقدمة في تكوين وإصدار القرارات الإدارية، مع وجوب مراعاة حماية حقوق الأفراد والمصلحة العامة، وتوفير آليات قانونية تمكن من مراجعة القرارات المؤتمتة، ووضع آلية واضحة للتظلم من تلك القرارات في حال وجود أخطاء فيها.

[20] – دعاء محمد إبراهيم، الأتمتة ودورها في دعم صناعة القرار الإداري من الناحية الإدارية والقانونية، مرجع سابق، ص74.

ولتنفيذ هذه الآلية لابد من توافر عنصر الشفافية الذي يتيح للمرفق العام العلم بمعطيات عمل الخوارزميات التي تتولى إصدار قرارات تخصه، بما يكفل حقه في الطعن عليها، في حالة وجود ضرر على مركزه القانوني، سواء بوقوع فعل، أو امتناع عن فعل، أو تعديله، وإلى جانب عنصر الشفافية لابد من توافر عنصر المسؤولية الإدارية، الذي يجعل الإدارة تتحمل المسؤولية عن الأضرار الناجمة عن القرارات الصادرة من جهتها، سواء معيبة بعيب شكلي أو عيب موضوعي.

1- الشفافية.

يعد مبدأ الشفافية من أهم مبادئ التي تتبعها الإدارة في سبيل تحقيق الحكم الرشيد، وتعرف على أنها: "مبدأ خلق بيئة تكون فيها المعلومات المتعلقة بالظروف والقرارات والأعمال الحالية المتاحة ومنظورة ومفهومة وبشكل أكثر تحديداً ومنهجياً في توفير المعلومات وجعل القرارات المتصلة بالسياسة معلومة للجميع من خلال النشر في الوقت المناسب والانفتاح لكل الأطراف ذوي العلاقة"[21].

وفي القرار الإداري العادي تكون متحققة نسبياً، ولكن في القرار الإداري المؤتمت تكون شبه مختفية داخل الأنظمة الإلكترونية، مما يجعل أمر فهمها وتقييم تطابقها مع القانون أمراً بالغ الصعوبة بالنسبة للمواطن العادي عند التعامل مع الجهات الإدارية الخوارزمية.

2- المسؤولية.

مواكبة الإدارة المحلية لتطورات الذكاء الاصطناعي عموماً ولتطبيقات الخوارزمية يضع على عاتقها العديد من المسؤوليات لضمان الاستغلال الأمثل والآمن لهذه التكنولوجيا، وأول هذه المسؤوليات ضرورة الالتزام بالتمكين الإداري للموظفين القائمين على البرنامج، من خلال تدريبهم وإقامة ورشات عمل وإنشاء ندوات لتزويدهم بالمعلومات حولها، ولتعزيز قدرتهم الفعلية على تسيير البرامج الخوارزمية [22].

الفرع الثاني: المعوقات القانونية التي تواجه تطبيق الأتمتة على القرارات الإدارية.

مع تزايد اعتماد الإدارات العامة على الخوارزميات في اتخاذ القرارات الإدارية، أصبح من الضروري تقييم مدى توافق هذه القرارات مع المبادئ القانونية الأساسية، لا سيما مبدأ المشروعية وحماية حقوق الأفراد، فالقرارات الإدارية المؤتمتة قد تكون أكثر كفاءة وسرعة، لكنها في الوقت ذاته قد تثير تحديات قانونية تتعلق بشرعيتها ومدى التزامها بالقوانين النافذة.

أولاً: إشكالية خضوع القرارات الإدارية المؤتمتة لرقابة المشروعية.

في أوروبا ألزمت اللائحة العامة لحماية البيانات (GDPR) المؤسسات بضرورة تبرير القرارات التي يتم اتخاذها بواسطة الخوارزميات، ومنح الأفراد حق الاعتراض عليها أو المطالبة بمراجعتها من قبل جهة

21 – سائدة الكيلاني، باسم سكجها، نحو شفافية أردنية، ط1، مؤسسة الأرشيف، عمان، 2000، ص16.

22– أيمن عودة المعاني، الإدارة العامة الحديثة، الطبعة الرابعة، دار وائل، للنشر والتوزيع ،2015 ، ص142.

بشرية، وهذا التوجه القانوني نحو ضمان استبدال القرار البشري بقرار آلي غير خاضع للرقابة القانونية، كما أصدرت بعض المحاكم الأوروبية أحكاماً تنص على ضرورة توفير "تفسير منطقي للقرارات الإدارية التي يتم اتخاذها بشكل آلي، حتى يتمكن الأفراد من الطعن فيها في حال كانت غير عادلة أو تنتهك حقوقهم[23].

أما في التشريعات العربية، فلا تزال التشريعات الخاصة بمشروعية القرارات الإدارية المؤتمتة محدودة، ومع ذلك بدأت بعض الدول في تطوير أطر قانونية تضمن التزام هذه القرارات بالمبادئ القانونية، حيث تشترط بعض الأنظمة ضرورة إشراف العنصر البشري على القرارات الإدارية المهمة، مثل قرارات التوظيف، والقبول في الجامعات، ففي السعودية تم تبني لوائح لتنظيم الذكاء الاصطناعي في القطاعات الحكومية والخاصة، حيث أصدرت "سياسة البيانات الوطنية"، التي تضع ضوابط لاستخدام الذكاء الاصطناعي في القرارات الإدارية، وتلزم الجهات الحكومية بضمان دقة القرارات الآلية وشفافيتها[24].

وفي ليبيا صدر القرار رقم (40) لسنة 2025م، باعتماد البرنامج الوطني للذكاء الاصطناعي والتحول الرقمي، وجاء في المادة 1 "يعتمد بموجب أحكام هذا القرار البرنامج الوطني للذكاء الاصطناعي والتحول الرقمي بليبيا، ويتمتع بالشخصية الاعتبارية والذمة المالية المستقلة، وتكون تبعيته لمركز الاتصال الحكومي، وتحت الاشراف المباشر لوزير الدولة للاتصال والشؤون السياسية"[25].

ثانياً: معوقات تحقيق الشفافية في ظل أنظمة الصندوق الأسود.

تعمل أنظمة الذكاء الاصطناعي بآلية معقدة للغاية حيث تقوم هذه الأنظمة بتعليم ذاتها بنفسها وتقوم باتخاذ القرارات بشكل مستقل بشكل لم يعد حتى بإمكان مبرمجيها الوقوف على الأسباب الحقيقية لاتخاذ هذه القرارات وتعرف هذه الظاهرة بظاهرة الصندوق الأسود والمقصود من وراء هذه التسمية أن النظام البرمجي يكون كصندوق أسود مصمت لا يمكن فهم ما بداخله ولا تفسير سلوكه، ولعل ذلك يبرز العديد من المشاكل القانونية تأتي في مقدمتها النية هي أحد الأركان الرئيسية في القرار الإداري، فإن الأصل

---

[23] – قانون حماية البيانات الأوروبي لسنة 2018، متوفر على الموقع الالكتروني: https://gdpr.eu/what-is-gdpr/ تاريخ الدخول: 2026/2/27.

[24] – غريسي صدوقي، رضا سي الطيب الهاشمي، علي العبسي، واقع وأهمية التحول الرقمي والأتمتة، مجلة أراء للدراسات الاقتصادية والادارية، الجزائر، المجلد 3، العدد 2، المركز الجامعي أفلو، 2021، ص100. متوفر على الموقع الالكتروني: https://asjp.cerist.dz/en/article/173522 تاريخ الدخول: 2026/2/25.

[25] – قرار مجلس الوزراء رقم (40) لسنة 2025 بشأن اعتماد البرنامج الوطني للذكاء الاصطناعي والتحول الرقمي في ليبيا، متوفر على الموقع الالكتروني: https://lawsociety.ly/legislation/%D9%82%D8%B1%D8%A7%D8%B1-%D9%85 تاريخ الدخول 2026/2/28.

كقاعدة عامة – أن الغاية من وراء أي قرار إداري هو تحقيق المصلحة العامة، وبالتالي فإن عبء إثبات العكس يقع على المدعي أي الطرف المتضرر [26].

وقد تصدى المجلس الدستوري الفرنسي لمسألة شفافية الخوارزميات المستخدمة وأتمتة القرار الإداري بشكل كامل في قضية (الكشف عن الخوارزميات التي تستخدمها مؤسسات التعليم العالي لاستعراض طلبات التسجيل في برامج الدراسة الجامعية لهذه الخوارزميات) قد أكد على تتعارض هذه الأحكام مع حق الوصول إلى المستندات الإدارية الصادر عن المادة 15من إعلان حقوق الإنسان والحقوق المدنية لعام 1789م[27].

ومن شأن هذه الأحكام أن تستبعد الوصول إلى الخوارزميات التي قد تستخدمها المؤسسات لمعالجة طلبات التسجيل للبرامج الدراسية المذكورة، والتي تم إدخالها باستخدام منصة "Parcoursup" الرقمية، ومع ذلك فإن مثل هذا الاستبعاد لن يكون له ما يبرره لا للحفاظ على سرية مداولات هيئات المحلفين التي تتعامل مع الطلبات، ولا لأي سبب آخر علاوة على ذلك، فإن هذه الأحكام تنتهك الحق في الحماية القانونية الفعالة لسببين. فمن ناحية، فإنها ستعيق التنفيذ الناجح للاستئناف ضد عدم الكشف عن المعلومات المعنية. ومن ناحية أخرى، من شأنه أن يحرم المتقاضين من العناصر اللازمة للطعن بفعالية في صحة رفض التسجيل[28].

ثالثاً: إشكالية تحيز البيانات.

ظاهر تحيز البيانات أو ما يسمي بالتحييز الخوارزمي التي تصف الأخطاء النظامية والمتكررة في نظم الحاسوب التي تؤدي إلى نتائج غير عادلة، مثل تفضيل مجموعة عشوائية من المستخدمين على المجموعات الأخرى، حيث أن من المعلوم أن تقنية الذكاء الاصطناعي لم تولد من فراغ بل أنها تستمد عملها من البيانات المدخلة لها والأنظمة والأكواد المنظمة لعملها، وهنا تظهر المشكلة حيث تتسلل ظاهرة تحييز البيانات إلي نظم الذكاء الاصطناعي بعدة طرق منها علي سبيل المثال: "**عملية تصميم البرنامج نفسه**" حيث يقوم المبرمج بإدراج بيانات من واقع خبرته الشخصية وانتماءاته ومعتقداته التي قد تؤدي إلي نتائج غير عادلة، وكان أمازون قد أثارت جدل واسع بخصوص هذا الأمر حيث قام قسم الموارد البشرية بشركة أمازون Amazon، البدء في عملية توظيف آلي كاملة حيث تم استخدام النماذج الرياضية

---

[26]– أحمد ناصر عباس، القرارات الإدارية المؤتمتة والسلطة التقديرية لجهة الإدارة، بحث مقدم للمؤتمر العلمي: التحديات والآفاق القانونية والاقتصادية للذكاء الاصطناعي، كلية الحقوق، جامعة عين شمس، مجلة العلوم القانونية والاقتصادية،2024، ص1142. متوفر على الموقع الالكتروني: https://jelc.journals.ekb.eg/article_342161_5997c57089eaefe2e48e9c7b7f8e6a7a.pdf تاريخ الدخول: 2026/2/28.

[27] – إعلان حقوق الانسان والمواطن لسنة 1789، منشور على الموقع الالكتروني: https://revolution.chnm.org/d/295 تاريخ الدخول 2026/3/1.

[28]– القرار رقم 834لسنة 2020، الصادر عن لجنة مراقبة الجودة (الاتحاد الوطني لطلاب فرنسا "الافصاح عن الخوارزميات المستخدمة من قبل مؤسسات التعليم العالي لمراجعة طلبات التسجيل في برامج الدراسة الجامعية وطبيعتها العامة)، للاطلاع متوفر على الموقع الالكتروني: https://www.conseil-constitutionnel.fr/en/decision/2020/2020834QPC.htm تاريخ الدخول: 2026/3/1.

«الخوارزميات >> التي تقوم عليها الأنظمة والتطبيقات العاملة بالذكاء الاصطناعي وتنحاز لفئة أو طرف ما أثناء عملها، على حساب فئة أو طرف أو أطراف أخرى، وذلك خلال قيامها بمهامها التي تبدأ بإجازة وترتيب وفرز البيانات ثم اتخاذ قرارات تتعلق بقبول خيارات معينة وتنفيذها ورفض خيارات أخرى واستبعادها من القائمة[29]، ومن ثم فان القرارات الإدارية المتخذة في هذا الشأن تكون غير منصفة ولا تسند إلى مبررات موضوعية، ومن أبرز القضايا على ظاهرة تحيز البيانات في بريطانيا هي التقديم للحصول على التأشيرات، حيث استخدمت وزارة الداخلية البريطانية خوارزميات لتكييف بيانات المتقدمين للحصول على التأشيرات وتحويلها إلى ألوان ورموز لتصنيف المتقدمين كعلامة على قبول المتقدم أو رفضه، فوجد ان النظام منحاز ضد جنسيات معينة فيتم رفضها دون فحص الملف من الأساس، الأمر الذي أدى الى إقامة دعوى قضائية لإلغاء النظام الخوارزمي لاتخاذ القرار لتحييز بياناته ضد جنسية معينة، وبالفعل صدر حكم من محكمة اول درجة بعدم مشروعية هذا النظام لتحيزه، وعلى اثره صدر قرار وزير الداخلية البريطاني بإلغاء النظام الذي يعمل بتقنية الأتمتة وذلك بسبب تحيزه ضد بعض الجنسيات دون وجود مبرر حقيقي[30]

المبحث الثاني: الحماية التقنية والجنائية للإدارة المحلية المؤتمتة كضمانة لاستدامتها.

مما لا شك فيه أن التحول الرقمي للإدارة المحلية يعد أحد الركائز الأساسية التي تسهم في تحسين جودة الخدمات المقدمة للمواطنين، وتعزيز التنمية المستدامة، فالتطور التكنولوجي وما يحسب له من انجاز المهام الإدارية بسرعة ودقة، جعل عمليات الأتمتة جزءاً لا يتجزأ من حوكمة الإدارة، تضمن تعزيز الكفاءة التشغيلية، وتقديم الخدمات للمواطنين بسرعة، بالتالي تقليل المعاملات الورقية، واختصار الوقت والجهد المستغرق في إنجازها، ويضاف إلى ذلك ضمان تحقيق مبدأ النزاهة والشفافية، من خلال مشاركة المواطنين في صنع القرار، ما يعزز الثقة بين المواطنين والإدارة.

وإن كانت أتمتة الإدارة المحلية ضرورة ملحة – كما أسلفنا القول– تمليها اعتبارات السرعة والكفاءة ورفع مستوى الإنجاز، من حيث تبسيط الإجراءات، وتحسين جودة الخدمات، بالتالي خلق جهاز إداري فعال يرتقي بوظائفه، ويقدم خدمات أكثر فاعلية، تبنى فيه القرارات على معطيات وبيانات تقنية، إلا أن ذلك سيفرز –من زاوية أخرى– تحديات جنائية معقدة، إذ أن الاعتماد المكثف على النظم الإلكترونية سيؤدي –

---

[29] – قرار أمازون بإلغاء أداة توظيف سرية تعمل بالذكاء الاصطناعي أظهرت تحيزاً ضد المرأة، منشور على الموقع الالكتروني: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G/ تاريخ الدخول 2026/3/1.

[30] – قرار وزارة الداخلية البريطانية بالتخلي عن خوارزمية "عنصرية من قرارات التأشيرة"، منشور على الموقع الالكتروني: https://www.bbc.com/news/technology-53650758 تاريخ الدخول 2026/3/2.

لا محالة– إلى نشوء أنماط من الجرائم يصعب كشفها، وتتبع مرتكبيها مالم يتم تحديث وتطوير آليات التحقيق والإثبات الجنائي بما يتماشى وطبيعة الجرائم الناشئة عن الاعتماد على النظم المؤتمتة.

وانطلاقا مما سبق، فإن تعزيز حماية الإدارة المحلية المؤتمتة يتطلب إقرار سياسة تجريمية وعقابية فعالة لردع السلوكيات الإجرامية وضبطها، وإن كان ذلك لا يكفي، بل يتطلب سياسة وقائية استباقية تتمثل في الحماية التقنية التي تمثل سياجا من الحماية للنظم الإلكترونية التي تعمل من خلالها الإدارة.

لكل ما تقدم سنحاول في هذا المبحث تسليط الضوء على آليات الحماية الفعالة للإدارة المحلية المؤتمتة من خلال تقسيمه إلى مطلبين، نخصص الأول لدراسة الوسائل التقنية لتأمين الإدارة المحلية المؤتمتة كخطوة استباقية على الحماية الجنائية، ونتناول في الثاني آليات الحماية الجنائية للإدارة المحلية المؤتمتة.

المطلب الأول: الوسائل الفنية التقنية لتأمين الإدارة المحلية المؤتمتة.

مما لا شك فيه أن أمن المعلومات يعد من أهم الركائز التي تأخذها الإدارة المحلية بعين الاعتبار لضمان استدامتها؛ لكونها تقلل إلى حد كبير من المخاطر والاعتداءات الإلكترونية التي تواجهها، من خلال تأمين وتحصين المنظومة الإلكترونية من الاعتداء عليها بأي شكل من الأشكال، بحيث يتم فرض سياج من الحماية الفعالة ضد التهديدات والهجمات السيبرانية، بما يحقق – في المحصلة – حماية البنية التحتية للشبكات والأجهزة والبيانات الحساسة، وضمان استمرارية الأعمال، والحفاظ على سمعة المرفق العام، وتعزيز الثقة الرقمية، ومنع الخسائر المالية، بالإضافة إلى الوصول الشرعي للبيانات من قبل الأشخاص المصرح لهم بالوصول إليها فقط [(31)]، ولا شك أن تلك الحماية لا تتحقق إلا بتبني منظومة متكاملة من الوسائل الفنية (ذات الطبيعة البشرية)، والتقنية (ذات الطبيعة التكنولوجية).

وقد أكدت الهيئة الوطنية لأمن وسلامة المعلومات على ذلك في قرارها رقم 44 لسنة 2021 بشأن اعتماد السياسات الوطنية لأمن وسلامة المعلومات [(32)]. وفيما يلي نتناول أهم الوسائل الفنية التقنية التي تلتزم الإدارة المحلية بتبنيها لحماية أنظمتها وبياناتها.

---

[31]– معن نايل محمود المعايطة، استراتيجيات الأمن السيبراني ودورها في تعزيز حماية الشبكات الإلكترونية في البلديات، مجلة العلوم الإنسانية والطبيعية، تصدر عن وزارة الإدارة المحلية، الأردن، المجلد (5)، العدد (4)، أبريل 2025، ص 366. (ص ص 362– 375)

[32]– قضت المادة الأولى في القرار المذكور بأن "تعتمد السياسات الوطنية لأمن وسلامة المعلومات وتعمم على كافة الوزارات والمؤسسات والشركات العامة والخاصة لتتولى تنفيذها والالتزام بها وتعميمها على الجهات التابعة لها لضمان أمن وسلامة المعلومات والبيانات الخاصة بها ضد التهديدات السيبرانية ...".

وأكد القرار على التزام الإدارة بتلك المعايير، فنص في المادة الثانية منه على أن "تلتزم كافة المؤسسات العامة والخاصة بوضع هذه السياسات موضع التنفيذ والتطبيق العملي لضمان سلامة معلوماتها وبياناتها". قرار رقم 44 لسنة 2021 بشأن اعتماد السياسات الوطنية لأمن وسلامة المعلومات، الهيئة الوطنية لأمن وسلامة المعلومات، الصادر في 16/ 12/ 2021.

الفرع الأول: الوسائل الفنية لتأمين لإدارة المحلية المؤتمتة.

وتتضن هذه الوسائل الإجراءات التي ترتبط بحسن استعمال النظم المعلوماتية وإدارتها داخل المرفق العام، ومن بينها يمكننا ذكر الآتي:

– **التوعية الأمنية للموظفين:** تعد التوعية الأمنية للموظفين أحد أهم الركائز الأساسية للأمن السيبراني [33]، من خلال توعيتهم بمخاطر التهديدات السيبرانية، وتثقيفهم بالممارسات الآمنة عبر الإنترنت، ولا شك أن هذه التوعية من شأنها أن تحول الموظف من كونه الحلقة الأضعف، إلى خط الدفاع الأول [34].

– **تعزيز التعاون والشراكات الاستراتيجية:** باعتبار أن التهديدات السيبرانية لا تعرف حدوداً جغرافية، فإن التعاون على الصعيدين الدولي والمحلي يعد ضرورة لا غنى عنها، لذلك فإن تأمين الحماية للإدارة المحلية يقتضي فتح آفاق التعاون بينها وبين المرافق الخاصة، وكذلك المجتمع المدني؛ لتبادل المعلومات، وتعزيز القدرة على التصدي للتهديدات والهجمات الإلكترونية، وكذلك انضمام ليبيا إلى الاتفاقيات الدولية المعنية بالأمن السيبراني، بالتالي الاستفادة من الخبرات العالمية، والحصول على الدعم الفني والتقني لمواجهة الهجمات العابرة للحدود [35].

– **اعتماد خطة الاستجابة للهجمات الإلكترونية داخل الإدارة:** لتأمين عمل الإدارة المؤتمتة يستوجب الأمر وضع خطة محددة وواضحة تبين الخطوات التي يجب اتخاذها للتصدي للهجمات، وتقليل المخاطر والأضرار، وتحديد الإجراءات اللازمة للتحقيق في الاعتداء وصولا إلى السبب الرئيسي، واستعادة العمليات الطبيعية في أسرع وقت ممكن [36].

---

[33]– يقصد بالأمن السيبراني توفير الحماية من الاستخدام غير المصرح به للبرامج والبيانات الإلكترونية، من خلال جملة من الإجراءات والضوابط والسياسات التقنية المصممة لحماية الشبكات والأجهزة الإلكترونية والبيانات من التهديدات السيبرانية. وقد عرفته وزارة الدفاع الأمريكية (البنتاغون) بأنه "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم سواء كانت: الهجمات، التجسس، التخريب والحوادث". للمزيد أنظر: جمال زمورة؛ ليلى بن عيسى، أهمية حوكمة الأمن السيبراني لضمان تحول رقمي آمن للخدمات العمومية في الجزائر، مجلة البحوث الاقتصادية المتقدمة، جامعة الوادي، الجزائر، المجلد 07، العدد 02، سبتمبر 2022، ص 416. (ص ص 414– 429)؛ حاتم بن عزوز؛ مناني حليمة، الأمن السيبراني والجريمة الإلكترونية في الدول ما بعد الحداثية: الولايات المتحدة نموذجا، مجلة الرسالة للدراسات الإعلامية، المجلد 06/ العدد 02/ جوان– يونيو، 2022. ص 581. (ص ص 580– 589)

[34]– أنظر: الأمن السيبراني ليبيا: دليلك الشامل لحماية مستقبلك الرقمي في 2025، مقالة منشورة على شبكة الانترنت، على الرابط الإلكتروني: Libya.rmg-sa.com.، تاريخ الزيارة: الخميس، 5 مارس 2026، الساعة 3:10 مساء.

[35]– أنظر: استراتيجية الأمن السيبراني: بناء حصن رقمي منيع لمستقبل واعد، 2025، مقالة منشورة على شبكة الانترنت، على الرابط الإلكتروني: Libya.rmg-sa.com.، تاريخ الزيارة: الخميس، 5 مارس 2026، الساعة 11:30 صباحا؛ سمير قلاع الضروس، الأمن السيبراني الوطني: قراءة في أهم الاستراتيجيات الأمنية والتقنية لمواجهة الجريمة الإلكترونية بالجزائر، مجلة الرواق للدراسات الاجتماعية والإنسانية، جامعة أحمد زبانة غليزان، الجزائر، المجلد 08، العدد 02، 2022، ص 262. (ص ص249– 267).

[36]– أنظر: فريق عمل نانو سوفت، الأمن السيبراني في ليبيا: حلول متكاملة لحماية أعمالك، أغسطس، 2025، مقالة منشورة على شبكة الانترنت، على الرابط الإلكتروني: nanosoft.ly، تاريخ الزيارة: الخميس، 5 مارس، 2026، الساعة 11:50 صباحا.

الفرع الثاني: الوسائل التقنية لتأمين الإدارة المحلية المؤتمتة.

إن تأمين الحماية بالوسائل التقنية لا يعني مجرد شراء برامج مكافحة الفيروسات فحسب، بل يقتضي أن يكون التأمين التقني عبارة عن منظومة متكاملة من وسائل الحماية، التي ترتكز على التكنولوجيا، التي ترمي إلى حماية النظم المعلوماتية من الاختراق، أو حتى من مجرد الوصول للبيانات، ومن بين هذه الوسائل ما يلي:

- **التشفير الإلكتروني [37]**: يعد التشفير وسيلة لتأمين البيانات المخزنة داخل النظم المعلوماتية، أو المرسلة عبر شبكة المعلومات الدولية، بالتالي ضمان سريتها وسلامتها من أي اختراق أو تطفل من شأنه أن يعرضها للتعديل أو التغيير [38].

وقد أكد المشرع على أن التشفير يعد وسيلة لحماية البيانات، وكذلك المعاملات الإلكترونية حينما قضى في المادة 58 من القانون رقم 6 لسنة 2022م بشأن المعاملات الإلكترونية بأن "يستخدم التشفير لحماية المعاملات الإلكترونية بهدف المحافظة على سرية المعلومات أو البيانات التي تحويها الرسالة الإلكترونية والتحقق من شخصية المنشئ، ومنع غيره من التقاط المعلومات أو الرسائل الإلكترونية بغرض منع وصولها إلى المرسل إليه أو تشويهها".

- **أنظمة التحكم في الوصول:** ويتم من خلال تلك الأنظمة التحقق من هوية المستخدم، وتطبيق سياسة الوصول، كما هو الحال في فرض كلمات مرور قوية على المستخدم يصعب كسرها، وكذلك التحقق البيومتري من شخصية المتعامل، وذلك بوسائل أجهزة القياس الحيوي، التي تعتمد على الخواص الذاتية، والصفات الفيزيائية، والجسدية والسلوكية، كما في البصمة الوراثية، وبصمة الإصبع، والشفاه، والبصمة القزحية "مسح العين"، والبصمة الصوتية "نبرة الصوت"، وبصمة الكف "خواص اليد" [39]. ويضاف لذلك

[37] – يقصد بالتشفير مجموعة من التقنيات التي تعمل على تحويل المعلومات إلى رموز تحول دون فهمها واستغلالها من قبل أشخاص غير مخولين بذلك، ما يضمن حماية المعلومات المرسلة إلى شخص أو جهة من أي تعديل، والحفاظ على خصوصيتها من أي اختراق. أنظر: تامر محمد سليمان الدمياطي، إثبات التعاقد الإلكتروني عبر الإنترنت، "دراسة مقارنة"، دار الكتب المصرية، القاهرة، الطبعة الأولى، 2009، ص 431.

وقد أكد المشرع الليبي على ذات المعنى حينما عرف التشفير بموجب القانون رقم 22 لسنة 2010 بشأن الاتصالات في المادة 1/ 19 منه، بأنه "استعمال رموز أو إشارات تصبح بمقتضاها المعلومات المراد ارسالها أو تمريرها غير قابلة للفهم من قبل الغير أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومة بدونها".

وعرفه ذات المشرع بموجب القانون رقم 5 لسنة 2022 المتعلق بمكافحة الجرائم الإلكترونية في المادة الأولى/ بند 5 بأنه "عملية تحويل البيانات الإلكترونية إلى رموز غير معروفة أو غير مفهومة يستحيل قراءتها أو معرفتها دون إعادتها إلى هيأتها الأصلية".

[38] – أنظر: أيسر صبري إبراهيم، إبرام العقد عن الطريق الإلكتروني وإثباته، "دراسة مقارنة"، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2015، ص 193.

[39]– أنظر: مروى محمد المودي، الدليل الرقمي في مجال الإثبات القضائي (دراسة مقارنة)، دار الجامعة الجديدة، الإسكندرية، الطبعة الأولى، 2024، ص 209– 210.

استخدام المصادقة متعددة العوامل، وهذه الوسيلة تضيف طبقة حماية قوية؛ لكونها تقتضي أن يقدم المستخدم دليلين على الأقل للتحقق من هويته، كأن يفرض عليه إدخال كلمة مرور ورمز على الهاتف [40].

– **تأمين الشبكات والبنية التحتية:** ويتحقق ذلك من خلال مجموعة من الوسائل التكنولوجية التي تعتمد على البرمجيات وأنظمة الحماية، من ذلك تطبيق جدار الحماية الناري، وهو عبارة عن مجموعة من البرمجيات والأجهزة التي تعمل على صد كل دخول غير مرخص به لنظام المعلومات من خلال تشكيل حدود فاصلة بين الشبكة الداخلية الخاصة بالمرفق العام، وشبكة الإنترنت العامة، بهدف التغلب على أكبر قدر ممكن من الثغرات الأمنية، من خلال بناء قناة اتصالات توجه إليها المعلومات المرسلة والمتبادلة مع شبكة الإنترنت؛ لمراقبتها والسيطرة على خروجها ودخولها من وإلى شبكة المرفق الخاصة [41].

ومن ذلك أيضا تأمين نقاط الوصول اللاسلكية (Wi–Fi) وتعمل هذه الوسيلة على منع الوصول غير المصرح به إلى الشبكة، من خلال مراقبة حركة المرور الشبكي [42].

كذلك أنظمة كشف الاختراق ومنع التسلل، التي تعمل على تسجيل جميع التعاملات التي تجري داخل موقع الحماية، وجميع الطلبات التي تأتي من خارجه، ثم تحليل المعلومات في سجلات الأحداث، فتحدد من خلال ذلك النشاطات غير النظامية؛ لذا تعد هذه الأنظمة فعالة في منع سرقة البيانات من قبل أي تهديد داخلي أو خارجي [43].

– **برامج مكافحة الفيروسات والبرمجيات الخبيثة:** وتعمل هذه البرامج على اكتشاف الفيروسات [44]، والبرامج الخبيثة كبرنامج التجسس، ومنعها من التسلل للشبكة، ومن إتلاف البيانات، من خلال مراقبة وتحليل

40– أنظر: الأمن السيبراني ليبيا: دليلك الشامل لحماية مستقبلك الرقمي في 2025، مرجع سبق ذكره.

41– أنظر: حديد نوفيل؛ حنان كريبط، أمن المعلومات ودوره في مواجهة الاعتداءات الإلكترونية على نظام معلومات المؤسسة، مجلة المؤسسة، جامعة الجزائر3، الجزائر، العدد3، 2014، ص 202. (ص ص 186– 207)؛ أنظر كذلك: عبد الوهاب بوبعة؛ عبد العالي لعور، دور الأمن المعلوماتي في مواجهة المخاطر التي تهدد نظام معلومات المؤسسة: دراسة حالة مؤسسة الإنجازات الكهربائية، مجلة الإدارة والتنمية للبحوث والدراسات، جامعة البليدة 2، الجزائر، المجلد 12، العدد 01، يونيو 2023، ص 222. (213– 232).

42 – أنظر: معن نايل محمود المعايطة، مرجع سبق ذكره، ص 369.

43– أنظر: حديد نوفيل؛ حنان كريبط، مرجع سبق ذكره، ص 204.

44 – الفيروس هو عبارة عن برنامج تخريبي تتم برمجته على أيدي محترفين، فيعمل من خلال إحداث خلل في خصائص الملفات التي يستهدفها؛ ليجعلها تحت سيطرة المبرمج، من خلال حذف جميع مستندات الملف أو تخريبها أو إدخال تعديل عليها، كل ذلك بهدف تخريب الجهاز الخاص بالمستخدم. للمزيد أنظر: حديد نوفيل؛ حنان كريبط، مرجع سبق ذكره، ص 202؛ كمال مسوس، ممارسات حوكمة أمن نظم المعلومات في المؤسسة: بين التقبل أو الحد من الاعتداءات الإلكترونية، المجلة الجزائرية للعولمة والسياسات الاقتصادية، مخبر العولمة والسياسات الاقتصادية، الجزائر، المجلد 13، 2022، ص 105. (ص ص 95 – 116).

الملفات، وتحطيم كل البرامج التي تحتوي بصمات معرفة بالبرنامج الخبيث أو بالفيروس؛ ولضمان فعالية هذه البرامج، ينبغي تحديثها باستمرار [45].

- **النسخ الاحتياطي للبيانات:** هذه الآلية تضمن حماية الإدارة أو المؤسسة من فقدان البيانات الخاصة بها ضد الهجمات السيبرانية، والأعطال الفنية المتوقعة، وغيرها، وإمكانية استعادتها بسهولة وسرعة في حالة فقدانها، بحيث تضع الجهة المعنية خطة نسخ احتياطي شاملة تحدد البيانات التي يجب نسخها احتياطيا، وعدد مرات النسخ، ومكان تخزين النسخ الاحتياطية، مع اختبار عملية استعادة البيانات للتحقق من عملها بشكل صحيح [46].

المطلب الثاني: آليات الحماية الجنائية للإدارة المحلية المؤتمتة.

إن الحماية الجنائية للإدارة المحلية المؤتمتة تستوجب – بالضرورة – الانتقال من حماية المحرر التقليدي الذي يأخذ شكل الورقة المكتوبة، إلى حماية منظومة رقمية ترتكز على بيانات إلكترونية، وهذه الأخيرة تعد أساس تقديم الخدمة، وركيزة القرار الإداري، ما يجعل الاعتداء عليها يشكل مساسا بحقوق الأفراد من جهة، وبالمصلحة العامة التي تهدف إلى انتظام المرفق العام من جهة أخرى.

الفرع الأول: تجريم الأفعال الماسة بالإدارة المحلية المؤتمتة.

إن صور الجرائم الماسة بالنظم المعلوماتية تتنوع بتنوع الوسائط الإلكترونية؛ الأمر الذي يفرض عليها– بما يتسع له المقام في هذا البحث– أن ننتهج معالجة انتقائية لأخطرها أثرا على الإدارة المحلية المؤتمتة، وخدماتها الوظيفية، وتهديدا لاستدامتها التقنية، وذلك كما نظمها المشرع في القانون رقم 5 لسنة 2022 المتعلق بمكافحة الجرائم الإلكترونية.

أولا: الجرائم الماسة بالأنظمة المؤتمتة.

وتتمثل الأفعال الإجرامية التي تستهدف الأنظمة المؤتمتة التي تعمل من خلالها الإدارة المحلية فيما يلي:

1- جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي للإدارة.

يعد الدخول أو البقاء في النظام المعلوماتي بشكل غير مشروع (بدون وجه حق) من أخطر الجرائم التي تقع على النظم المعلوماتية، بالنظر لما يترتب عليها من مخاطر جمة، فالدخول غالبا ما يشكل الخطوة الأولى لنشاطات إجرامية أخرى تلحق به، كما لوكان بهدف الاطلاع على المعلومات التي يحتويها ذلك

---

[45]– أنظر: عبد الوهاب بوبعة؛ عبد العالي لعور، دور الأمن المعلوماتي في مواجهة المخاطر التي تهدد نظام معلومات المؤسسة: دراسة حالة مؤسسة الإنجازات الكهربائية، مرجع سابق، ص 222. (213- 232).

[46] – أنظر: فريق عمل نانو سوفت، الأمن السيبراني في ليبيا: حلول متكاملة لحماية أعمالك، مرجع سبق ذكره.

مجلة العلوم الشاملة العدد 40 ـــ
ويقصد بالدخول غير المشروع: قيام الفاعل بالدخول إلى النظام المعلوماتي دون أن يكون مسموحا له بذلك، كما لو كان الدخول من قبل أحد موظفي الإدارة، لكنه يختص بالدخول للنظام في مجال قسمه دون الأقسام الأخرى [48].

أما البقاء: فيقصد به مكوث الفاعل داخل النظام المعلوماتي فترة من الوقت يزيد عما هو مسموح به، أو تجاوز الوقت المسموح به للبقاء [49].

لكل ذلك نجد أن المشرع قد حرص على تجريم كل دخول غير مصرح به إلى النظم المعلوماتية، وكذلك كل تواجد أو بقاء بدون تصريح، بعد أن كان دخوله مشروعا، وتقوم الجريمة بمجرد الدخول أو البقاء غير المصرح به (أي الولوج إلى البيانات أو المعلومات بدون رضا المسؤول عن النظام)، بصرف النظر عن النتيجة التي تترتب على ذلك الدخول أو البقاء، إذ أن النتيجة التي تترتب على ذلك الدخول غير المشروع، يكون لها أثر في مقدار العقوبة فحسب لا في التجريم [50]، وهو ما ورد في المادة 12 من القانون رقم 5 لسنة 2022م أعلاه.

2- اختراق الأنظمة وقواعد البيانات

لم ترد جريمة اختراق الأنظمة في القانون الليبي كجريمة مستقلة، بل وردت كوسيلة من وسائل الدخول غير المشروع الواردة في المادة 11 من القانون رقم 5 لسنة 2022م. ويقصد بالاختراق "القدرة على الوصول إلى أي وسيلة تقنية للمعلومات بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاصة"[51].

والاختراق بالمفهوم المتقدم يعد طريقة أو وسيلة من وسائل الدخول غير المشروع، ككسر كلمة المرور، أو استخدام برمجيات للاختراق، أو استغلال ثغرات النظام الأمنية، بالتالي فكل اختراق يعد دخولا غير مشروع، ولكن ليس كل دخول غير مشروع يعد اختراقا، حيث يتصور أن يكون الدخول غير مشروع دون أن يعد اختراقا، كأن يستخدم شخص كلمة مرور خاصة بالغير دون إذنه مثلا. ما يعني أن الدخول

---

[47]- تنص المادة 11 من القانون المذكور على أن "يعد الدخول لأجهزة أو أنظمة الحاسب الآلي أو إلى نظام معلوماتي أو شبكة معلوماتية أو موقع إلكتروني غير مشروع إذا تم الاختراق بشكل متعمد لوسائل وإجراءات الحماية لها بشكل كلي أو جزئي دون تصريح أو بما يخالف التصريح".

[48]- أنظر: محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الإلكترونية، مكتبة الوفاء القانونية، الإسكندرية، الطبعة الأولى، 2014، ص 380 وما يليها.

[49] - أنظر: صليحة بن عودة، الجريمة الإلكترونية وأثرها على مشروعية أعمال الإدارة القانونية، مجلة دفاتر الحقوق والعلوم السياسية، المجلد 03، العدد 1، 2023، ص 53. ص ص (45- 60).

[50] - أنظر: خديجة بن موسى، الحماية الجنائية للمعطيات في المجال المعلوماتي، بحث مقدم ضمن متطلبات نيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة غرداية، الجزائر، 2021/ 2022م، ص 33.

[51]- المادة الأولى/ بند 2 من القانون رقم 5 لسنة 2022 المتعلق بمكافحة الجرائم الإلكترونية.

غير المشروع أوسع نطاقا في مضمونه من الاختراق، وما الاختراق إلا طريقة أو وسيلة يتم بها ذلك الدخول.

3- تعطيل عمل النظام أو الخدمات الرقمية الحكومية.

لقد أفرد المشرع نصا خاصا يتعلق بتعطيل الأعمال الحكومية باستخدام الوسائل الإلكترونية، وذلك في المادة 34 من القانون رقم 5 لسنة 2022م [52]، حيث اعتبر المشرع أن الجريمة تتحقق بقيام الجاني بتعطيل سير العمل داخل الإدارة، أو عرقلته وارباكه، وذلك باستخدام أي وسيلة إلكترونية، كما لو قام بتعطيل النظام الإلكتروني للإدارة المحلية، أو تعطيل موقعها الإلكتروني، أو إيقاف خدمات الدفع الإلكتروني التابعة لها، أو تعطيل الشبكة المعلوماتية المرتبطة بها، وإعاقة الوصول إلى الخدمة، أو التشويش عليها.

وقد اعتبر المشرع أن هذه الجريمة تعد من الجرائم الإلكترونية الخطرة؛ بالنظر لما ينجم عنها من تعطيل الخدمات الرقمية للإدارة، وإرباك سير العمل، وتهديد أمنه واستقراره؛ لذا شدد العقوبة على مرتكبها، ضمانا لحماية استمرارية الإدارة، وسهولة وسرعة انجاز العمل داخلها.

ثانيا: الجرائم الواقعة على البيانات والمعلومات الرقمية.

من أهم الجرائم التي يكون محلها البيانات أو المعلومات الرقمية، والتي تعمل الإدارة المحلية المؤتمتة من خلالها، يمكن ذكر الآتي:

1- انتهاك سرية البيانات أو المعلومات الشخصية وسلامتها.

قد تنتج جريمة انتهاك سرية وسلامة البيانات في الغالب على دخول النظام المعلوماتي دون وجه حق، أو بشكل غير مشروع، ويتمثل سلوك انتهاك السرية في افشاء البيانات الخاصة أو نشرها، ما يعرض صاحبها لأضرار جسيمة، سواء كان الأخير شخصا طبيعيا أو معنويا، إذ قد تصل الأضرار التي تلحق بالشخص الطبيعي جراء إفشاء سرية بياناته إلى حد إفساد استقرار حياته وحياة أسرته. كما يعرض إفشاء أسرار الشخص المعنوي إلى اهتزاز ثقة الناس في الإدارة، وزوالها ربما [53].

أما انتهاك سلامة البيانات أو المعلومات الخاصة فيقصد به تعريض تلك البيانات أو المعلومات للخطر، كما لو تم تدميرها ومحوها، أو تغييرها، أو نقلها، أو إدخال تعديلات عليها دون وجه حق بالحذف، أو بالإضافة [54].

52- تقضي المادة المذكورة أعلاه بأن "يعاقب ... كل من عطل الأعمال الحكومية أو أعمال السلطة العامة أو قام بعرقلتها باستعمال أي وسيلة إلكترونية.

ويعاقب بالعقوبة ذاتها كل من أنتج أو زرع أو حاز برامج معدة لهذا الاستعمال".

53 – أنظر: ما شاء الله عثمان الزوي، المسؤولية الجنائية للدخول أو البقاء غير المشروع في النظام المعلوماتي: دراسة مقارنة في القانون الليبي المقارن، المجلة العربية للدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، 2023، ص 142، ص ص (139- 152)

54- أنظر: ما شاء الله عثمان الزوي، مرجع سبق ذكره، ص 143.

وقد أكد المشرع على حماية سرية البيانات وسلامتها بموجب نص المادة 12 من القانون رقم 5 لسنة 2022م [55].

2- التلاعب بالبيانات الإدارية لتحقيق منافع دون وجه حق.

مما لا شك فيه أن البيانات التي تعتمد عليها الإدارة المؤتمتة تعد من أهم الأصول الرقمية التي يتم بها تسيير المرافق العامة، وتقوم عليها عملية اتخاذ القرار الإداري، ولأهمية تلك الأصول فإن أي عبث بها، أو تعديل لمحتواها بطريقة غير مشروعة يعد مساسا بسلامة العمل الإداري وبموثوقية مخرجاته.

وتتحقق الجريمة المذكورة بقيام الجاني بإدخال أو حذف أو تعديل، أو تغيير البيانات المخزنة داخل النظام المعلوماتي التابع للإدارة دون وجه حق، أو تغيير حقيقتها، وذلك بقصد تحقيق منفعة شخصية، أو منفعة للغير [56].

وقد تناول المشرع حالة خاصة من حالات التلاعب بهدف تحقيق منفعة شخصية، أو منفعة للغير، وذلك في المادة 40 من القانون رقم 5 لسنة 2022م، والتي جرم فيها المشرع فعل التلاعب بالبيانات الطبية الرقمية، كتعديل نتائج التحاليل أو التقارير الطبية، أو اتلاف البيانات الصحيحة المخزنة إلكترونيا أو إخفائها، أو تسهيل التلاعب للغير من خلال تمكينه من تغيير أو اخفاء البيانات خلافا للمشروعية [57].

3- سرقة أو كشف البيانات الخاصة بالمواطنين أو بالموظفين.

يقصد بسرقة البيانات: أن يأخذ الجاني نسخة من تلك البيانات، ويدخلها في حيازته كما هي، دون أن يؤثر على أصل تلك البيانات بأي شكل من الأشكال [58].

فهي كل فعل غير مشروع يتحقق بالحصول على بيانات الأفراد الخاصة (أدوات التعريف والهوية) [59] المخزنة في النظم المعلوماتية التابعة للإدارة دون وجه حق، ويتحقق ذلك من خلال نسخ تلك البيانات، أو استخراجها من النظام واستعمالها أو نقلها دون ترخيص قانوني بذلك، أو بيعها أو تسريبها للغير.

55- "وتكون العقوبة ... إذا كان الدخول بقصد إلغاء أو حذف أو إضافة أو تدمير أو افشاء أو إتلاف أو حجب أو تعديل أو نقل أو نسخ بيانات أو تعطيل عمل نظام معلومات أو تغيير موقع إلكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو انتحال شخصية مالكه.

فإذا نجم عن الدخول إعاقة عمل النظام المعلوماتي أو تعطيل الشبكة المعلوماتية أو عمل الموقع الإلكتروني أو إفساد محتوياتهم تكون العقوبة ..."

56- لقد أكد المشرع على ذلك بموجب المادة 15 من القانون رقم 5 لسنة 2022م التي تنص على أن "يعاقب ... كل من قام بصورة غير مشروعة بإلحاق ضرر مادي بغيره عن طريق إدخال أو تبديل أو محو أو تدمير بيانات معلوماتية بأي شكل من أشكال التعدي على عمل نظام معلوماتي للحصول دون وجه حق على منفعة مادية لنفسه أو لغيره".

57- تنص المادة 40 على أن "يعاقب بالسجن كل من أتلف الفحوص الطبية أو التشخيص الطبي أو العلاجي أو الرعاية الطبية أو عدل فيها بما يخالف حقيقتها أو أخفى نتائجها دون مبرر. أو سهل فعل ذلك باستعمال شبكة المعلومات الدولية أو بأي وسيلة إلكترونية أخرى".

58 – أنظر: ما شاء الله عثمان الزوي، مرجع سبق ذكره، ص 143.

59- لقد تولى المشرع تعريف هذين المصطلحين ضمن المادة الأولى من القانون رقم 5 لسنة 2022م المتعلقة بالتعريفات، فعرف أدوات التعريف والهوية في البند 9 بأنها "أي آلية أو نظام رقمي أو أداة رقمية تستخدم لتمثيل الهوية الرقمية للأفراد التي تمكنهم من العمل بطريقة آمنة مع واجهات استخدام متناسقة على الأنظمة المختلفة على المعلومات الدولية".

أما كشف البيانات فيقصد به إفشاؤها، أو تمكين الآخرين من الاطلاع عليها دون ترخيص، أو دون إذن الجهة التي تملكها، والكشف أو التسريب يعد مخالفا في مفهومه لمفهوم السرقة، حيث تقوم الأخيرة على الاستيلاء أو الحصول على البيانات دون وجه حق، أما الأولى فتنصرف في معناها إلى إفشاء البيانات أو إتاحتها للغير دون إذن الجهة المالكة لها، بالتالي قد يتحقق الكشف دون سرقة، كما لو قام الفاعل بالوصول إلى البيانات بصورة مشروعة بحكم وظيفته التي تخوله ذلك، ثم قام بإفشائها، أو اتاحتها للغير.

لا شك أن سرقة البيانات الشخصية المحفوظة لدى الإدارة، أو كشفها تمس مساسا صارخا بسريتها وخصوصيتها، سواء كانت تتعلق بالمعطيات الإدارية، أو المالية، أو التعريفية، أو الوظيفية، وجميع ما ذكر يعد من أكثر المعلومات حساسية ؛ لذا يحرص المشرع دائما على تقرير حماية جنائية صريحة للبيانات الشخصية، والحيلولة دون الاستيلاء عليها بأي طريق غير مشروع، أو نسخها أو كشفها للغير دون مبرر قانوني، والقول بخلاف ذلك سيؤثر سلبا على الثقة داخل الإدارة المؤتمتة، وفي قدرتها على حماية البيانات الشخصية التي عهد إليها بها من جانب المواطنين والموظفين على حد سواء، وما تقدم يفهم من استقراء نص المادة 18 من القانون رقم 5 لسنة 2022م [60].

4- اعتراض البيانات المنقولة بغير إذن، والتنصت على الاتصالات الإلكترونية المتبادلة.

لقد حرص المشرع الليبي على تجريم فعل الاعتراض والتعرض للبيانات في المادة 13 من القانون رقم 5 لسنة 2022م [61]، والتنصت غير المشروع بموجب المادة 47 من ذات القانون [62].

وقد أفرد المشرع لكل من الاعتراض والتنصت مادتين مستقلتين عن بعض بالنظر لاختلاف مفهوم كل منها، وكذلك اختلاف محل الحماية الذي قصده المشرع حين جرمهما، فيقصد بالاعتراض كما ورد في المادة الأولى/ 12 بأنه "مشاهدة البيانات أو المعلومات أو الحصول عليها". وهو بهذا المفهوم يرد على البيانات الرقمية أو المعلومات المتبادلة عبر النظم المعلوماتية من خلال الاطلاع عليها، والاعتداء على تدفقها داخل النظام، والحيلولة دون بلوغها وجهتها، بالتالي المساس بسريتها وسلامتها.

---

60 – "يعاقب .... كل من قام بالاستيلاء على أدوات التعريف والهوية العائدة لشخص آخر المستخدمة في نظام معلوماتي.

ويعاقب ... كل من قام بصورة غير مشروعة مع علمه بالأمر باستخدام أدوات التعريف والهوية العائدة إلى شخص آخر في نظام معلوماتي".

61 – "يعاقب ... كل من اعترض نظاما معلوماتيا بقصد الحصول على بيانات رقمية أو للربط مع أنظمة إلكترونية أخرى".

62 – "يعاقب ... كل من تنصت لصالح نفسه أو لصالح غيره على الاتصالات التي تجرى عبر شبكة المعلومات الدولية أو أي وسيلة إلكترونية أخرى.

وتكون العقوبة السجن إذا كان التنصت بقصد الحصول على أسرار حكومة أمنية أو عسكرية أو مصرفية.

فإذا نشر الأسرار المذكورة بالفقرة السابقة عبر شبكة المعلومات الدولية أو أي وسيلة إلكترونية أخرى أو مكن شخصا أو جهة أخرى من الحصول عليها تكون العقوبة السجن المؤبد".

أما التنصت فلم يرد له تعريفا في القانون أعلاه، ومع ذلك يمكن تعريفه كما قصده المشرع ضمن قانون العقوبات الليبي (63)، وما جرى عليه العمل القضائي، بأنه الاستماع أو الاطلاع خلسة على محادثات مكتوبة أو مسموعة، أو الاستماع – دون إذن قانوني – للمراسلات بجميع أشكالها (64) أثناء تداولها أو نقلها فيما بين أصحاب المصلحة، أو تخزينها داخل النظام المعلوماتي، فالتنصت يرد على الاتصالات أو المحادثات الخاصة بالأشخاص، ما يشكل اعتداء على خصوصيتها، بالتالي على حرمة الحياة الخاصة.

الفرع الثاني: التشديد العقابي على الأفعال الماسة بالإدارة المحلية المؤتمتة.

في إطار الحماية الجنائية للإدارة المحلية المؤتمتة، انتهج المشرع سياسة التشديد العقابي على الأفعال التي تستهدف البيانات، والنظم المعلوماتية التي تعتمد عليها الإدارة في تقديم الخدمات وأداء المهام، وتقوم تلك السياسة على اعتبارات عدة، منها ما يستند فيه المشرع على القصد الجنائي لدى الجاني، وما يعكسه من خطورة إجرامية لديه، ومنها ما يقوم على جسامة النتائج أو الأضرار التي قد تنجم عن الفعل الإجرامي، وتفصيل ذلك كالآتي:

أولا: التشديد وفقا للقصد الجنائي لدى الجاني:

يعد القصد الجنائي من أهم المعايير التي يعتمدها المشرع في تقرير التشديد العقابي، ويتجلى هذا المسلك في بعض النصوص القانونية التي أوردها ضمن القانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية، ففي المادة 2/12 ربط المشرع التشديد بالقصد الجنائي، فقضى بأن تشدد العقوبة إذا كان الدخول بقصد إلغاء أو حذف أو إضافة، أو تدمير أو افشاء أو إتلاف، أو حجب أو تعديل أو نقل، أو نسخ بيانات أو تعطيل عمل نظام معلومات، أو تغيير موقع إلكتروني، أو إلغائه أو إتلافه أو تعديل محتوياته، أو انتحال شخصية مالكه، فقرر وفقا للقصود المذكورة فرض عقوبة وجوبية تتمثل في الحبس لمدة لا تقل عن سنة، وغرامة لا تقل عن خمسمائة دينار ولا تزيد عن خمسة آلاف دينار. وذلك بعد أن كانت العقوبة المقررة للجريمة في صورتها البسيطة عقوبة تخييرية تتمثل في الحبس لمدة لا تزيد عن سنة، أو بغرامة لا تقل عن مائة دينار ولا تزيد عن خمسمائة دينار، أو العقوبتين معا، لكل من دخل لأجهزة أو أنظمة الحاسب الآلي أو نظام معلوماتي أو شبكة معلوماتية أو موقع إلكتروني.

63– تقضي المادة 244 من قانون العقوبات الليبي في فقرتها الثانية بأن "...يراد من ((الرسالة)) المكاتيب والمحادثات التليفونية والبرقيات وما إلى ذلك من وسائل الارسال".

64– عرف المشرع الليبي مصطلح الاتصالات في القانون رقم 22 لسنة 2010 بشأن الاتصالات في المادة الأولى بأنه "كل عملية نقل أو بث أو إرسال للرموز أو الإشارات أو الأصوات أو الصور أو البيانات أيا كانت طبيعتها بواسطة الوسائل السلكية واللا سلكية أو أي وسيلة من وسائل تقنية الاتصالات"، وهذا ما يعني أن المراسلات تشمل المكالمات الهاتفية عبر الانترنت، والرسائل النصية، ورسائل الوسائط المتعددة، والبريد الإلكتروني، وغيرها من الوسائل المستحدثة التي تستخدم في تبادل المعلومات عبر الشبكات الرقمية، للمزيد أنظر: عثمان مذكور، الحماية الجنائية لحرمة المراسلات الإلكترونية في القانون الليبي والفرنسي، مجلة جامعة فزان العلمية، ليبيا، المجلد الخامس، العدد الأول، 2026، ص 397. (ص ص 393- 414).

وذات المسلك انتهجه المشرع في المواد 16، و18، من ذات القانون، فقرر في المادة 16 عقوبة الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن ألف دينار ولا تزيد على عشرة آلاف دينار لكل من قام بصورة غير مشروعة، بإدخال أو تبديل أو محو أو تدمير بيانات معلوماتية نتج عنها بيانات غير صحيحة، بقصد استخدامها أو التعويل عليها في أغراض قانونية كما لو كانت هذه البيانات صحيحة.

وتزاد العقوبة لكل من قام باستعمال تلك البيانات المعلوماتية، مع علمه بعدم صحتها، حيث يعاقب بالسجن، وبغرامة لا تقل عن ألف دينار، ولا تزيد على عشرة آلاف دينار.

أما في المادة 18، ففرض عقوبة الحبس مطلقا، والغرامة التي تتراوح ما بين ألف دينار، وثلاثة آلاف دينار، على كل من قام بالاستيلاء على أدوات التعريف والهوية الخاصة بالغير، والمستخدمة في نظام معلوماتي. في حين تشدد العقوبة على الجاني متى قام بصورة غير مشروعة مع علمه بذلك باستخدام أدوات التعريف والهوية العائدة إلى شخص آخر في نظام معلوماتي.

كما شدد المشرع في عقوبة التنصت غير المشروع بموجب المادة 47، وذلك وفقا للقصد الجنائي للجاني، فقرر للجريمة في صورتها البسيطة عقوبة الحبس لمدة لا تقل عن سنة لكل من تنصت لصالح نفسه أو لصالح غيره على الاتصالات التي تجرى عبر شبكة المعلومات الدولية، أو أي وسيلة إلكترونية أخرى.

ويصف المشرع الجريمة ذاتها بالجناية إذا كانت التنصت غير المشروع بقصد الحصول على أسرار حكومية أو أمنية، أو عسكرية، أو مصرفية، فقرر لها عقوبة السجن مطلقا، بحيث لا تقل مدة السجن عن ثلاث سنوات، ولا تتجاوز خمس عشرة سنة، ويترك للقاضي أمر تفريد العقوبة بما يتناسب مع ظروف الفعل وملابساته.

وتشدد العقوبة عن ذات الجريمة إلى حد السجن المؤبد، وذلك إذا قصد الجاني من فعل التنصت نشر المعلومات والأسرار التي تحصل عليها، أو مكّن شخصا أو جهة أخرى من الحصول عليها.

ثانيا: التشديد وفقا لجسامة النتائج التي تنجم عن الفعل الإجرامي:

لا يقتصر التشديد العقابي لتحقيق الحماية الجنائية للإدارة المحلية المؤتمتة على معيار القصد الجنائي لدى الفاعل فحسب، بل قد يستند في ذلك التشديد على جسامة النتائج التي يفضي إليها السلوك الإجرامي، بمعنى النظر للآثار السلبية الضارة الناتجة عن الجرائم التي تهدد المصالح المحمية جنائيا، وهدف المشرع من تغليظ العقوبة هنا إلى تحقيق مبدأ التناسب ما بين جسامة الضرر ومقدار العقوبة، ويمكننا تبين سياسة التشديد العقابي وفقا لجسامة النتيجة باستقراء نص المادة 3/12، حيث يشدد فيها المشرع العقوبة بحسب ما تفضي إليه النتيجة التي تنجم عن السلوك، وما تتسبب فيه من أضرار للنظام المعلوماتي، فقرر عقوبة وجوبية لا تخييرية، تتمثل في السجن والغرامة التي لا تقل عن عشرة آلاف دينار، إذا نجم عن الدخول

إعاقة عمل النظام المعلوماتي، أو تعطيل الشبكة المعلوماتية أو عمل الموقع الإلكتروني، أو إفساد محتوياتهم، بالتالي أضفى على الجريمة وصف الجناية بعد أن كانت جنحة.

الخاتمة.

في ختام هذا البحث يتضح أن الأتمتة أصبحت من أهم الأدوات الحديثة التي تسهم في تطوير الإدارة المحلية وتعزيز استدامتها، لما توفره من إمكانات كبيرة في تحسين كفاءة العمل الإداري وتسريع إنجاز المعاملات وتقليل الأخطاء البشرية. كما أن اعتماد الأنظمة المؤتمتة يسهم في تعزيز الشفافية والحد من مظاهر الفساد الإداري، من خلال توثيق الإجراءات الإدارية وإتاحة إمكانية الرقابة والمتابعة بشكل أكثر دقة، كما تساعد الأتمتة في كشف المخالفات والجرائم الإدارية والمالية، وتسهيل عمليات التحقيق والمساءلة القانونية بفضل حفظ البيانات وتسجيل العمليات بصورة منظمة.

ومن أبرز النتائج:

- إن استخدام الأتمتة يدعم اتخاذ القرار الإداري من خلال توفير بيانات دقيقة تساعد القيادات المحلية على التخطيط الاستراتيجي بشكل أفضل.
- تعد الأتمتة أداة قوية وهامة لدفع عجلة الإدارة المحلية نحو التطوير وتحسين جودة الخدمات للمواطنين، غير أن ضمان استدامتها يستوجب تعزيز الحماية الفعالة التكاملية من خلال استراتيجية تقنية، وسياسة جنائية حديثة.
- وجود تحديات تعيق التطبيق الكامل للأتمتة ، مثل ضعف البنية التحتية التقنية، وقلة الكفاءات البشرية المتخصصة ومحدودية التمويل في بعض الإدارات المحلية.
- إن تعزيز استدامة الإدارة المحلية يقتضي تطبيق سياسة أمن قوية تضمن الامتثال لمعايير وضوابط الأمن السيبراني.
- إن إجراءات الحماية التقنية والجنائية للإدارة المحلية المؤتمتة تعد ضرورة ملحة، ليس فقط لحماية بيانات المواطنين، بل أكثر من ذلك للحفاظ على الثقة العامة في نظم الأتمتة الحديثة.

التوصيات:

- ضرورة تطوير البنية التحتية بالتقنية اللازمة لتطبيق الأتمتة في مؤسسات الإدارة المحلية.
- الاستمرار في دعم مشاريع التحول الرقمي لتحقيق إدارة محلية أكثر كفاءة واستدامة.
- الحرص على تحديث القوانين واللوائح باستمرار ؛ لمواكبة التحديث السريع للتكنولوجيا الحديثة، وما ينجم عنها من تهديدات واعتداءات مستحدثة. ووضع سياسات وإجراءات للحماية الفعالة ضد الهجمات السيبرانية داخل الإدارة المحلية بهدف تعزيز استدامتها ورفع كفاءة الخدمات التي تقدمها للمواطنين

- ضرورة الإسراع في سن قانون يعنى بمكافحة الجرائم الإلكترونية كمنظومة متكاملة، بحيث لا يقف المشرع عند حد تنظيم الشق الموضوعي فحسب، لأن ذلك يجعل النصوص غير ذات جدوى، بل ينبغي بالإضافة لذلك أن ينظم الجوانب الإجرائية المتعلقة بالملاحقة بما يضمن وضع النصوص الموضوعية موضع التنفيذ، والحرص على ذلك إنما يتأتى من الطبيعة الرقمية اللا مادية التي تتسم بها الأدلة الرقمية.

قائمة المراجع.

أولاً الكتب:

- أحمد بن محمد الهرماس الشمري، أثر وسائل الاتصال الإلكترونية في نفاذ القرارات الإدارية، مجلة البحوث القانونية والاقتصادية، 2020.
- أيسر صبري إبراهيم، إبرام العقد عن الطريق الإلكتروني وإثباته، "دراسة مقارنة"، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2015.
- أيمن عودة المعاني، الإدارة العامة الحديثة، الطبعة الرابعة، دار وائل، للنشر والتوزيع ،2015 .
- تامر محمد سليمان الدمياطي، إثبات التعاقد الإلكتروني عبر الإنترنت، "دراسة مقارنة"، دار الكتب المصرية، القاهرة، الطبعة الأولى، 2009.
- حسن عواد السريحي، وآخرون: أتمتة أعمال المكاتب (دراسة تطبيقية على إمارة مكة المكرمة)، دار المريخ للنشر والتوزيع، الرياض، المملكة العربية السعودية، 1999م.
- خالد سمارة الزعبي، تشكيل المجالس المحلية، مكتبة دار الثقافة، عمان، ط3، 1993.
- سعد غالب ياسين، الإدارة الإلكترونية وأفاق تطبيقاتها العربية، مركز الإدارة العام، المملكة العربية السعودية، 2005.
- علاء عبد الرازق السالمي، محمد عبدالعال النعيمي، أتمتة المكاتب، الطبعة الأولى، دار المناهج للنشر والتوزيع، الرياض، 1999.
- سائدة الكيلاني، باسم سكجها، نحو شفافية أردنية، ط1، مؤسسة الأرشيف، عمان، 2000، ص16.
- سعد غالب ياسين، نظم مساندة القرار، دار المناهج، عمان، 2006.
- محمد حمدي الطعامنة، طارق العلوش، الحكومة الالكترونية في الدول العربية، المنظمة العربية للتنمية الإدارية، القاهرة، 2004.

- مروى محمد المودي، الدليل الرقمي في مجال الإثبات القضائي (دراسة مقارنة) ، دار الجامعة الجديدة، الإسكندرية، الطبعة الأولى، 2024.
- محمد نور برهان، الموارد البشرية في الفنادق، دار الصفاء للنشر والتوزيع، عمان، 1998.
- محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الإلكترونية، مكتبة الوفاء القانونية، الإسكندرية، الطبعة الأولى، 2014.

ثانياً: الرسائل العلمية:

- خديجة بن موسى، الحماية الجنائية للمعطيات في المجال المعلوماتي، بحث مقدم ضمن متطلبات نيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة غرداية، الجزائر، 2021/ 2022م.
- عبدالله حسن العبد القادر، توطين تقنية المعلومات في دول مجلس التعاون الخليجي نحو إدارة مثلى، رسالة ماجستير، غير منشورة، جامعة الملك فهد للبترول والمعادن، الرياض، 2000.
- ناصر بن منيف العتيبي، الأتمتة ودورها في تحسين أداء إدارات الموارد البشرية في الأجهزة الأمنية بمدينة الرياض، رسالة دكتوراه، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الإدارية الرياض، 2007.

ثالثاً: البحوث والمقالات العلمية:

- أحمد ناصر عباس، القرارات الإدارية المؤتمتة والسلطة التقديرية لجهة الإدارة، بحث مقدم للمؤتمر العلمي: التحديات والآفاق القانونية والاقتصادية للذكاء الاصطناعي، كلية الحقوق، جامعة عين شمس، مجلة العلوم القانونية والاقتصادية ،2024. متوفر على الموقع الالكتروني: https://jelc.journals.ekb.eg/article_342161_5997c57089eaefe2e48e9c7b7f8e6a7a.pdf تاريخ الدخول: 2026/2/28.
- بخيث مبارك الراشدي، أثر الأتمتة على تحسين قيادة المؤسسات، مجلة المعرفة، المغرب، العدد الثلاثون، 2025، ص184.
- بوبعة عبد الوهاب؛ عبد العالي لعور، دور الأمن المعلوماتي في مواجهة المخاطر التي تهدد نظام معلومات المؤسسة: دراسة حالة مؤسسة الإنجازات الكهربائية، مجلة الإدارة والتنمية للبحوث والدراسات، جامعة البليدة 2، الجزائر، المجلد 12، العدد 01، يونيو 2023.
- جمال زمورة؛ ليلى بن عيسى، أهمية حوكمة الأمن السيبراني لضمان تحول رقمي آمن للخدمات العمومية في الجزائر، مجلة البحوث الاقتصادية المتقدمة، جامعة الوادي، الجزائر، المجلد 07، العدد 02، سبتمبر 2022.

- حاتم بن عزوز؛ مناني حليمة، الأمن السيبراني والجريمة الإلكترونية في الدول ما بعد الحداثية: الولايات المتحدة نموذجا، مجلة الرسالة للدراسات الإعلامية، المجلد 06/ العدد 02/ جوان– يونيو، 2022.
- حديد نوفيل؛ حنان كريبط، أمن المعلومات ودوره في مواجهة الاعتداءات الإلكترونية على نظام معلومات المؤسسة، مجلة المؤسسة، جامعة الجزائر 3، الجزائر، العدد 3، 2014.
- سمير قلاع الضروس، الأمن السيبراني الوطني: قراءة في أهم الاستراتيجيات الأمنية والتقنية لمواجهة الجريمة الإلكترونية بالجزائر، مجلة الرواق للدراسات الاجتماعية والإنسانية، جامعة أحمد زبانة غليزان، الجزائر، المجلد 08، العدد 02، 2022.
- صليحة بن عودة، الجريمة الإلكترونية وأثرها على مشروعية أعمال الإدارة القانونية، مجلة دفاتر الحقوق والعلوم السياسية، المجلد 03، العدد 1، 2023.
- دعاء محمد إبراهيم، الأتمتة ودورها في دعم صناعة القرار الإداري من الناحية الإدارية والقانونية، مجلة الكوفة للعلوم القانونية والسياسية، جامعة الكوفة، كلية القانون، العراق، المجلد 17، العدد 59، 2024، ص67.
- علاء محي الدين مصطفى أبو أحمد، القرار الإداري الإلكتروني، مجلة البحوث القانونية والاقتصادية، 2015، العدد 25 (42).
- عثمان يوسف محمد العبيد، دور الأتمتة الرقمية في البلدية للدوائر الإدارية، المالية والفنية، مجلة رماح للبحوث والدراسات، 2022، العدد٦٦.
- عثمان مذكور، الحماية الجنائية لحرمة المراسلات الإلكترونية في القانون الليبي والفرنسي، مجلة جامعة فزان العلمية، ليبيا، المجلد الخامس، العدد الأول، 2026.
- غريسي صدوقي، رضا سي الطيب الهاشمي، علي العبسي، واقع وأهمية التحول الرقمي والأتمتة، مجلة أراء للدراسات الاقتصادية والادارية، الجزائر، المجلد 3، العدد 2، المركز الجامعي أفلو، 2021، ص100. متوفر على الموقع الالكتروني: https://asjp.cerist.dz/en/article/173522 تاريخ الدخول: 2026/2/25.
- كمال مسوس، ممارسات حوكمة أمن نظم المعلومات في المؤسسة: بين التقبل أو الحد من الاعتداءات الإلكترونية، المجلة الجزائرية للعولمة والسياسات الاقتصادية، مخبر العولمة والسياسات الاقتصادية، الجزائر، المجلد 13، 2022.

- ما شاء الله عثمان الزوي، المسؤولية الجنائية للدخول أو البقاء غير المشروع في النظام المعلوماتي: دراسة مقارنة في القانون الليبي المقارن، المجلة العربية للدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، 2023.
- معن نايل محمود المعايطة، استراتيجيات الأمن السيبراني ودورها في تعزيز حماية الشبكات الإلكترونية في البلديات، مجلة العلوم الإنسانية والطبيعية، تصدر عن وزارة الإدارة المحلية، الأردن، المجلد (5)، العدد (4)، أبريل 2025.
- محمد البداوي، القرار الإداري الإلكتروني، مجلة المنارة للدراسات القانونية والإدارية، 2018، العدد 23.
- الأمن السيبراني ليبيا: دليلك الشامل لحماية مستقبلك الرقمي في 2025، مقالة منشورة على شبكة الانترنت، على الرابط الإلكتروني: .Libya.rmg-sa.com، تاريخ الزيارة: الخميس، 5 مارس 2026، الساعة 3:10 مساء.
- استراتيجية الأمن السيبراني: بناء حصن رقمي منيع لمستقبل واحد، 2025، مقالة منشورة على شبكة الانترنت، على الرابط الإلكتروني: .Libya.rmg-sa.com، تاريخ الزيارة: الخميس، 5 مارس 2026، الساعة 11:30 صباحا.
- فريق عمل نانو سوفت، الأمن السيبراني في ليبيا: حلول متكاملة لحماية أعمالك، أغسطس، 2025، مقالة منشورة على شبكة الانترنت، على الرابط الإلكتروني: nanosoft.ly، تاريخ الزيارة: الخميس، 5 مارس، 2026، الساعة 11:50 صباحا.

رابعاً: التشريعات والمواثيق.

- القانون الليبي رقم 22 لسنة 2010 بشأن الاتصالات. منشور على الموقع الالكتروني: **https://security-legislation.ly/ar/latest-laws/%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%B1**
- القانون رقم 5 لسنة 2022 المتعلق بمكافحة الجرائم الإلكترونية : منشور على الموقع الالكتروني: https://lawsociety.ly/legislation/%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%B1%
- قانون العقوبات الليبي لسنة 1953، منشور على الموقع الالكتروني: **https://security-legislation.ly/ar/latest-laws/%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%**
- القرار رقم 44 لسنة 2021 بشأن اعتماد السياسات الوطنية لأمن وسلامة المعلومات، الهيئة الوطنية لأمن وسلامة المعلومات، الصادر في 16/ 12/ 2021. متوفر على الموقع الالكتروني:

https://lawsociety.ly/legislation/%D9%82%D8%B1%D8%A7%D8%B1-%D8%B1%D9%82

- قانون حماية البيانات الأوروبي لسنة 2018، متوفر على الموقع الالكتروني: https://gdpr.eu/what-is-gdpr/ تاريخ الدخول: 2026/2/27.
- قرار مجلس الوزراء رقم (40) لسنة 2025 بشأن اعتماد البرنامج الوطني للذكاء الاصطناعي والتحول الرقمي في ليبيا، متوفر على الموقع الالكتروني: https://lawsociety.ly/legislation/%D9%82%D8%B1%D8%A7%D8%B1-%D9%85 تاريخ الدخول 2026/2/28.
- USAID, DESIGNING AND IMPLEMENTING COURT AUTOMATION PROJECTS Practical Guidance for USAID DRG Officers August 2019, accessible on: https://www.usaid.gov/sites/default/files/2022-05/USAID-CAP-Guide FINAL.pdf تاريخ الدخول 2026/2/24.
- إعلان حقوق الانسان والمواطن لسنة 1789، منشور على الموقع الالكتروني: https://revolution.chnm.org/d/295 تاريخ الدخول 2026/3/1.
- قرار أمازون بإلغاء أداة توظيف سرية تعمل بالذكاء الاصطناعي أظهرت تحيزاً ضد المرأة، منشور على الموقع الالكتروني: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G/ تاريخ الدخول 2026/3/1.
- قرار وزارة الداخلية البريطانية بالتخلي عن خوارزمية "عنصرية من قرارات التأشيرة"، منشور على الموقع الالكتروني: https://www.bbc.com/news/technology-53650758 تاريخ الدخول 2026/3/2 .
- القرار رقم 834لسنة 2020، الصادر عن لجنة مراقبة الجودة (الاتحاد الوطني لطلاب فرنسا "الافصاح عن الخوارزميات المستخدمة من قبل مؤسسات التعليم العالي لمراجعة طلبات التسجيل في برامج الدراسة الجامعية وطبيعتها العامة)، للاطلاع متوفر على الموقع الالكتروني:

https://www.conseil-constitutionnel.fr/en/decision/2020/2020834QPC.htm تاريخ الدخول: 2026/3/1.