

The Legal Framework for Protecting Public Funds from Cyberattacks: Balancing National Security Requirements and the Protection of Public Services

Munay Mohammed Awadh Omar*
Independent Researcher, Al-Marj, Libya

النظام القانوني لحماية الأموال العامة من الهجمات السيبرانية بين متطلبات الأمن القومي
وحماية المرفق العام

منى محمد عوض عمر*
باحثة مستقلة، المرج، ليبيا

*Corresponding author: idreasomar2010@gmail.com

Received: July 08, 2026	Revised: September 04, 2026	Accepted: September 15, 2026
	Published: September 23, 2026	

Abstract:

This study examines the legal framework for protecting public funds from cyberattacks in Libya, emphasizing national security and the continuity of public utilities. It assesses the adequacy of existing legislation and institutional arrangements in addressing cyber threats arising from the digital management of public funds and services. A descriptive-analytical approach is employed to examine relevant provisions of the Libyan Civil Code, economic crimes legislation, cybercrime and electronic transactions laws, and the 2026 decision establishing the National Authority for Cybersecurity and Digital Sovereignty. The findings indicate that effective protection must extend beyond traditional public funds to encompass associated digital assets, platforms, systems, and data. Although Libyan legislation provides important protective mechanisms, their dispersion across multiple laws limits legal coherence and highlights the need to clarify the legal status of public digital assets. Cyberattacks affecting critical institutions and infrastructure may disrupt essential services and threaten economic stability and national security. Consequently, cybersecurity is closely linked to the regularity and continuity of public utilities. Establishing the National Authority represents a significant shift toward preventive institutional protection through risk management, supervision, and incident response. The study recommends an integrated, proactive national cybersecurity framework incorporating critical infrastructure classification, mandatory incident reporting, improved digital evidence rules, business continuity and recovery planning, and stronger coordination among judicial, security, financial, and regulatory authorities. Such measures would strengthen the protection of public funds, sustain essential services, and safeguard national security and digital sovereignty.

Keywords: Public Funds, Cyberattacks, Cybersecurity, National Security, Public Utilities, Cybercrime, Digital Sovereignty.

المخلص:

تتناول هذه الدراسة الإطار القانوني لحماية الأموال العامة من الهجمات السيبرانية في ليبيا، مع التركيز على متطلبات الأمن القومي واستمرارية المرافق العامة. وتهدف إلى تقييم مدى كفاية التشريعات والترتيبات المؤسسية القائمة في مواجهة التهديدات السيبرانية الناشئة عن الإدارة الرقمية للأموال والخدمات العامة. وتعتمد الدراسة المنهج الوصفي التحليلي من

خلال فحص الأحكام ذات الصلة في القانون المدني الليبي، وتشريعات الجرائم الاقتصادية، وقوانين مكافحة الجرائم الإلكترونية والمعاملات الإلكترونية، والقرار الصادر سنة 2026 بإنشاء الهيئة الوطنية للأمن السيبراني والسيادة الرقمية. وتشير النتائج إلى أن الحماية الفعالة يجب أن تتجاوز الأموال العامة بمفهومها التقليدي لتشمل الأصول والمنصات والأنظمة والبيانات الرقمية المرتبطة بها. ورغم توفير التشريعات الليبية آليات مهمة للحماية، فإن تشتتها بين قوانين متعددة يحد من التكامل التشريعي، ويبرز الحاجة إلى توضيح الوضع القانوني للأصول الرقمية العامة. كما قد تؤدي الهجمات السيبرانية التي تستهدف المؤسسات والبنية التحتية الحيوية إلى تعطيل الخدمات الأساسية وتهديد الاستقرار الاقتصادي والأمن القومي. وعليه، يرتبط الأمن السيبراني ارتباطاً وثيقاً بانتظام سير المرافق العامة واستمراريتها. ويُمثل إنشاء الهيئة الوطنية تحولاً مهماً نحو الحماية المؤسسية الوقائية القائمة على إدارة المخاطر والإشراف والاستجابة للحوادث. وتوصي الدراسة بإرساء إطار قانوني وطني متكامل واستباقي للأمن السيبراني، يشمل تصنيف البنية التحتية الحيوية، والإبلاغ الإلزامي عن الحوادث، وتطوير قواعد الأدلة الرقمية، ووضع خطط لاستمرارية الأعمال والتعافي، وتعزيز التنسيق بين الجهات القضائية والأمنية والمالية والرقابية؛ بما يدعم حماية الأموال العامة، ويضمن استمرارية الخدمات الأساسية، ويصون الأمن القومي والسيادة الرقمية.

الكلمات المفتاحية: الأموال العامة، الهجمات السيبرانية، الأمن السيبراني، الأمن القومي، المرفق العام، الجرائم الإلكترونية، السيادة الرقمية.

المقدمة:

شهد العالم خلال العقود الأخيرة تحولاً متسارعاً نحو الرقمنة والاعتماد على تقنيات المعلومات والاتصالات في إدارة شؤون الدولة وتقديم الخدمات العامة وإدارة الموارد المالية والاقتصادية، حتى أصبحت الأنظمة الإلكترونية وقواعد البيانات والمنصات الرقمية جزءاً أساسياً من البنية المؤسسية للمرافق العامة. ولم يعد استخدام التكنولوجيا مقتصرًا على تسهيل الإجراءات الإدارية، بل امتد إلى إدارة الحسابات العامة، والموازنات، والتحويلات المصرفية، والإيرادات والنفقات، والمشتريات والعقود الحكومية، والسجلات المالية والضريبية والجمركية، وغيرها من المجالات المرتبطة بصورة مباشرة أو غير مباشرة بالأموال العامة. وقد ترتب على ذلك انتقال جانب مهم من المال العام من بيئة مادية تقليدية إلى بيئة رقمية مترابطة، الأمر الذي أوجد صوراً جديدة للاعتداء عليه تتجاوز الوسائل التقليدية المعروفة في القانون.

وتحظى الأموال العامة بحماية قانونية خاصة بالنظر إلى ارتباطها الوثيق بتحقيق المصلحة العامة واستمرار الدولة في أداء وظائفها؛ فالمال العام لا يستمد أهميته من قيمته المالية وحدها، وإنما من تخصيصه للمنفعة العامة واتصاله بنشاط المرافق العامة. ومن ثم، أقامت التشريعات قواعد استثنائية لحمايته مدنياً وإدارياً وجنائياً، انطلاقاً من أن الاعتداء عليه لا يمس دمة مالية عادية فحسب، وإنما يمكن أن ينعكس على قدرة الدولة على تمويل خدماتها وتنفيذ سياساتها وتحقيق أهدافها الاقتصادية والاجتماعية. وفي النظام القانوني الليبي، حظيت الأموال العامة بحماية دستورية ومدنية وجنائية، كما ارتبطت صفة المال العام أساساً بتخصيصه للمنفعة العامة، وهو ما يجعل حمايته في جوهرها حماية للمصلحة العامة وللنشاط الذي يؤديه المرفق العام (الغزير، 2017، ص ص 261-295؛ الكيلاني، 2025).

غير أن التحول الرقمي أفرز نوعاً مختلفاً من المخاطر التي تهدد الأموال العامة، يتمثل في الهجمات السيبرانية الموجهة إلى الأنظمة والشبكات وقواعد البيانات التي تعتمد عليها الجهات العامة في إدارة أموالها ومرافقها. فقد أصبح من الممكن أن يقع الاعتداء على المال العام من خلال اختراق الأنظمة المالية، أو التلاعب بالسجلات والبيانات، أو الاستيلاء غير المشروع على الأموال عبر الوسائط الإلكترونية، أو تعطيل أنظمة الدفع والتحويل، أو تشفير البيانات وطلب الفدية، أو اختراق حسابات الجهات العامة، أو تعطيل البنى التحتية الرقمية التي تعتمد عليها المرافق الحيوية. وبذلك لم تعد حماية المال العام مرتبطة فقط بمنع الاختلاس أو الاستيلاء أو الإضرار المادي به، وإنما أصبحت تقتضي كذلك حماية البيئة الرقمية التي يُدار المال العام من خلالها.

وتزداد خطورة هذه الاعتداءات عندما تستهدف الأموال أو البيانات أو الأنظمة التابعة للمرافق العامة الحيوية؛ إذ قد لا تتوقف آثار الهجوم السيبراني عند حدود الخسارة المالية المباشرة، وإنما يمكن أن تؤدي إلى تعطيل الخدمات العامة والإخلال بمبدأ استمرارية المرفق العام، فضلاً عن المساس بثقة الأفراد في الإدارة ومؤسسات الدولة. ولهذا أصبحت البنية التحتية المعلوماتية جزءاً أساسياً من بنية المرافق العامة الحديثة، وأصبحت حمايتها من المخاطر السيبرانية مرتبطة بضمان الاستمرارية والانتظام والأمن في تقديم الخدمات العامة. وقد ذهب اتجاه حديث في الدراسات القانونية العربية إلى النظر إلى الأمن السيبراني نفسه باعتباره وظيفة عامة حديثة تتصل بحماية النظام الرقمي العام، وتخضع في تنظيمها لمتطلبات الاستمرارية والعمومية وإشراف الدولة (عبد الوهاب وآخرون، 2026).

ولا ينفك أثر الهجمات السيبرانية عند حدود حماية المرفق العام، بل يمتد إلى الأمن القومي للدولة، ولا سيما عندما تستهدف الهجمات قطاعات استراتيجية مثل المصارف والطاقة والاتصالات والنقل والمالية العامة والمؤسسات السيادية. فالاعتماد المتزايد على الشبكات والأنظمة الرقمية أدى إلى اتساع مفهوم الأمن القومي ليشمل إلى جانب أبعاده التقليدية بُعداً سيبرانياً يرتبط بحماية المعلومات والبيانات والبنى التحتية الرقمية والاقتصاد الوطني من المخاطر التي يمكن أن تهدد استقرار الدولة أو تعطل مؤسساتها. ومن هذا المنظور، لم يعد الهجوم على النظام الإلكتروني لمرفق مالي أو اقتصادي

مجرد جريمة تقنية منفردة، وإنما قد يتحول، بالنظر إلى طبيعته وحجمه والجهة المستهدفة وآثاره، إلى تهديد للأمن الاقتصادي والسيبراني والقومي للدولة.

وتبدو هذه المسألة أكثر أهمية في الحالة الليبية؛ فقد تناولت دراسات حديثة أثر التهديدات السيبرانية في الأمن القومي الليبي، وأشارت إلى تعرض مؤسسات ليبية ذات طبيعة اقتصادية واستراتيجية لهجمات سيبرانية، ومن بينها مؤسسات مرتبطة بالقطاع المالي والنفطي، بما يؤكد أن المخاطر السيبرانية يمكن أن تتجاوز أمن المعلومات بمعناه الفني إلى التأثير في المصالح الاقتصادية والاستراتيجية للدولة (عصمان، 2025).

وفي مواجهة هذه التحولات، لم يعد التنظيم القانوني للأمن السيبراني مسألة تقنية بحتة، وإنما أصبح جزءاً من السياسة التشريعية للدولة في حماية المال العام والمرافق العامة والأمن القومي. ويتطلب ذلك وجود منظومة قانونية متكاملة تجمع بين قواعد حماية الأموال العامة، وقواعد التجريم والعقاب، وتشريعات المعاملات والبيانات الإلكترونية، والقواعد المنظمة للمرافق العامة، فضلاً عن تحديد اختصاصات الجهات المكلفة بالوقاية والاستجابة للحوادث السيبرانية والتحقيق فيها واستعادة الأنظمة والبيانات المتضررة.

وفي هذا السياق، يمثل القانون الليبي رقم (5) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية إحدى الأدوات التشريعية المهمة في مواجهة الاعتداءات الواقعة في البيئة الرقمية؛ إذ استهدف حماية التعاملات الإلكترونية وتحقيق الأمن المعلوماتي وحماية الاقتصاد الوطني والحقوق المترتبة على الاستخدام المشروع للتقنيات الحديثة وتعزيز الثقة في سلامة المعاملات الإلكترونية، كما قرر عدداً من صور التجريم والعقاب المرتبطة بالاعتداء على الأنظمة والبيانات والأدلة الرقمية (قانون مكافحة الجرائم الإلكترونية الليبي رقم 5 لسنة 2022).

وقد شهد التنظيم المؤسسي الليبي تطوراً أكثر حداثة بصدر قرار مجلس الوزراء رقم (358) لسنة 2026 بشأن إنشاء الهيئة الوطنية للأمن السيبراني والسيادة الرقمية، الذي أسند إليها وضع السياسات والاستراتيجيات والمعايير الوطنية للأمن السيبراني والسيادة الرقمية. ومن الأهمية بمكان أن القرار ربط صراحة بين تأمين البنية التحتية المعلوماتية ومواجهة مخاطر الهجمات السيبرانية وبين المحافظة على الأمن القومي واستقرار عمل مؤسسات الدولة، كما امتدت اختصاصات الهيئة إلى الجهات العامة والخاصة وما يتعلق بأمن وحماية المعلومات الرقمية والمصالح الليبية ذات الصلة (قرار مجلس الوزراء رقم 358 لسنة 2026، المواد 3-5).

ويكشف ذلك عن تطور في فلسفة الحماية القانونية؛ فالحماية التقليدية للأموال العامة تقوم أساساً على منع التصرف فيها أو الحجز عليها أو اكتسابها بالتقادم، إلى جانب تجريم صور الاختلاس والاستيلاء والإضرار بها، بينما تتطلب البيئة الرقمية الانتقال إلى الحماية الوقائية والاستباقية. وهذه الحماية لا تنتظر تحقق الاعتداء فعلياً، وإنما تقوم على إلزام الجهات العامة باتخاذ التدابير التقنية والتنظيمية والقانونية اللازمة لمنع الاختراق، وتأمين الأنظمة وقواعد البيانات، وتصنيف المعلومات، وإدارة المخاطر، ومراقبة الدخول إلى الأنظمة، والإبلاغ عن الحوادث، وضمان النسخ الاحتياطي واستمرارية الأعمال والتعافي بعد الهجمات.

ومن هنا تتداخل في حماية الأموال العامة من الهجمات السيبرانية ثلاث دوائر قانونية مترابطة: تتمثل الأولى في حماية المال العام ذاته بوصفه مآلاً مخصصاً لتحقيق المنفعة العامة؛ وتتعلق الثانية بحماية المرفق العام وضمان انتظامه واستمراره وعدم تعطيل خدماته نتيجة الاعتداء على بنيته الرقمية؛ بينما تتمثل الثالثة في حماية الأمن القومي عندما يترتب على الهجوم تهديد للاقتصاد الوطني أو المؤسسات السيادية أو البنية التحتية الحيوية أو الاستقرار العام للدولة. ويترتب على هذا التدخل أن المعالجة القانونية للهجوم السيبراني لا ينبغي أن تقتصر على وصفه باعتباره جريمة إلكترونية فحسب، وإنما يجب أن تراعي طبيعة المال محل الحماية، وصفة الجهة المستهدفة، ومدى اتصال النظام المعتدى عليه بمرفق عام، وحجم الآثار المترتبة على الأمن القومي.

كما يؤثر هذا الموضوع إشكالية تتعلق بمدى كفاية القواعد القانونية التقليدية المقررة لحماية المال العام في التعامل مع الاعتداءات السيبرانية الحديثة. فالقواعد التقليدية صيغت في الأصل لمواجهة صور الاعتداء المادي أو المالي المباشر، بينما يمكن للهجوم السيبراني أن يقع دون انتقال مادي للأموال، وأن يستهدف البيانات أو الأنظمة التي تحدد الحقوق المالية أو تدبير المال العام، كما قد يقع من خارج إقليم الدولة، أو باستخدام تقنيات تخفي هوية مرتكبيه، أو من خلال شبكات موزعة عبر أكثر من دولة. وهو ما يفرض إعادة النظر في نطاق الحماية القانونية من حيث محل الحماية، والمسؤولية، والاختصاص، والإثبات الرقمي، والتعاون المؤسسي والدولي.

وعليه، تنطلق هذه الدراسة من أن حماية الأموال العامة في العصر الرقمي لم تعد تتحقق بمجرد توفير الحماية المدنية والجنائية التقليدية، بل أصبحت تستلزم بناء نظام قانوني متكامل للأمن السيبراني يجمع بين الوقاية والتجريم والرقابة والاستجابة والتعافي، ويربط بين حماية المال العام وضمان استمرارية المرافق العامة والمحافظة على الأمن القومي. ومن هذا المنطلق تسعى الدراسة إلى تحليل مدى كفاية النظام القانوني القائم لمواجهة الهجمات السيبرانية التي تستهدف الأموال العامة، وبيان طبيعة العلاقة بين قواعد حماية المال العام ومتطلبات الأمن السيبراني، وتحديد مدى تأثير هذه الهجمات في استمرارية المرافق العامة، فضلاً عن الوقوف على حدود اعتبار حماية الأموال والأنظمة الرقمية التابعة للدولة أحد متطلبات حماية الأمن القومي في البيئة الرقمية المعاصرة.

وتتحدد الإشكالية المركزية للدراسة في التساؤل الآتي: إلى أي مدى يوفر النظام القانوني حماية فعالة للأموال العامة من الهجمات السيبرانية بما يحقق التوازن والتكامل بين متطلبات حماية الأمن القومي وضمان أمن واستمرارية المرفق العام؟

مشكلة الدراسة:

أدى التوسع في استخدام النظم الرقمية داخل مؤسسات الدولة والمرافق العامة إلى انتقال جانب كبير من عمليات إدارة الأموال العامة وتحصيلها وإنفاقها ومراقبتها إلى البيئة الإلكترونية، الأمر الذي أسهم في رفع كفاءة الأداء الإداري والمالي، إلا أنه أوجد في الوقت ذاته صوراً مستحدثة من المخاطر والاعتداءات التي قد تستهدف الأنظمة وقواعد البيانات والحسابات والمنصات المرتبطة بالمال العام. وأصبحت الهجمات السيبرانية من أبرز هذه المخاطر؛ لما يمكن أن يترتب عليها من استيلاء أو تحويل غير مشروع للأموال، أو تلاعب بالبيانات والسجلات المالية، أو تعطيل الأنظمة الإلكترونية، أو إتلاف المعلومات، أو المساس بسرية البيانات المرتبطة بالمؤسسات العامة.

وتتجاوز خطورة هذه الهجمات مجرد الإضرار بالقيمة المالية للأموال العامة؛ إذ قد يمتد أثرها إلى تعطيل المرافق العامة والإخلال بانتظامها واستمرارها، خاصة عندما تعتمد هذه المرافق على أنظمة إلكترونية في إدارة خدماتها ومواردها. كما تتضاعف الخطورة عندما تستهدف الهجمات قطاعات حيوية أو استراتيجية، مثل المالية والمصارف والطاقة والاتصالات والنفط، بحيث يصبح الاعتداء السيبراني مسألة تتصل بالأمن الاقتصادي والسيبراني للدولة، ومن ثم بالأمن القومي.

وتبرز المشكلة القانونية في أن الحماية التقليدية المقررة للأموال العامة نشأت أساساً لمواجهة صور الاعتداء المادي المعروفة، كاختلاس المال العام والاستيلاء عليه والإضرار به، في حين تتميز الهجمات السيبرانية بطبيعة مختلفة من حيث الوسيلة ومحل الاعتداء ومركبيه وأثارها وإثباتها، فضلاً عن إمكانية وقوعها عبر الحدود ومن دون وجود مادي للجاني في إقليم الدولة. وهو ما يثير التساؤل حول مدى قدرة قواعد حماية المال العام التقليدية على استيعاب هذه الصور الحديثة من الاعتداء.

وعلى الرغم من صدور القانون الليبي رقم (5) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية، إلى جانب القواعد القانونية المقررة لحماية الأموال العامة وتنظيم المعاملات الإلكترونية، فإن تعدد النصوص والجهات المعنية بالحماية يثير إشكالية بشأن مدى وجود نظام قانوني متكامل يجمع بين الحماية الوقائية والجنائية والإدارية والتقنية للأموال العامة، ويحدد بصورة واضحة مسؤوليات الجهات العامة عن تأمين أنظمتها وبياناتها، وآليات الاستجابة للهجمات السيبرانية، والمسؤولية المترتبة على الإخلال بمتطلبات الأمن السيبراني.

كما تثير الدراسة إشكالية تتعلق بحدود العلاقة بين ثلاثة اعتبارات قانونية متداخلة: حماية الأموال العامة من الاعتداء، وضمان انتظام المرفق العام واستمراره، والمحافظة على الأمن القومي للدولة. فالهجوم الإلكتروني الواحد قد يشكل اعتداءً على المال العام، وفي الوقت نفسه يؤدي إلى تعطيل مرفق عام، وقد يرتقي من حيث نطاقه وخطورته وأثاره إلى مستوى التهديد الذي يمس الأمن القومي. ومن ثم، تظهر الحاجة إلى تحديد الأساس القانوني الذي يحكم هذه الحالات ومدى كفاية التشريع القائم للتعامل معها بصورة متكاملة.

وعليه، تتمثل مشكلة الدراسة في بحث مدى كفاية وفاعلية النظام القانوني القائم في توفير الحماية للأموال العامة من الهجمات السيبرانية، ومدى قدرته على استيعاب الطبيعة المستحدثة لهذه الاعتداءات وتحقيق التكامل بين حماية المال العام ومتطلبات الأمن القومي وضمان استمرارية المرافق العامة، مع الكشف عن أوجه القصور أو الفراغ التشريعي واقتراح الآليات القانونية الكفيلة بتعزيز هذه الحماية.

التساؤل الرئيسي:

- إلى أي مدى يوفر النظام القانوني القائم حماية فعالة للأموال العامة من الهجمات السيبرانية بما يحقق متطلبات الأمن القومي ويضمن حماية المرفق العام واستمراره؟

ويتفرع عن هذا التساؤل الرئيس عدد من التساؤلات:

1. ما المقصود بالأموال العامة والهجمات السيبرانية، وما طبيعة الحماية القانونية المقررة للمال العام في البيئة الرقمية؟
2. ما مدى كفاية التشريعات الليبية القائمة، ولا سيما التشريعات المتعلقة بالجرائم الإلكترونية، في مواجهة الهجمات السيبرانية التي تستهدف الأموال العامة؟
3. ما أثر الهجمات السيبرانية الواقعة على الأموال والأنظمة العامة في مبدأ انتظام المرفق العام واستمراره؟
4. متى يرتقي الاعتداء السيبراني على الأموال أو الأنظمة التابعة للمرافق العامة إلى مستوى التهديد للأمن القومي؟
5. ما مدى تكامل الأدوار والمسؤوليات بين الجهات القانونية والإدارية والفنية المختصة بحماية الأموال العامة والأمن السيبراني؟
6. ما أوجه القصور التشريعي والمؤسسي في النظام القانوني القائم، وما الآليات التي يمكن اعتمادها لتعزيز حماية الأموال العامة من الهجمات السيبرانية؟

أولاً: أهداف الدراسة:

تهدف هذه الدراسة بصورة رئيسة إلى تحليل النظام القانوني لحماية الأموال العامة من الهجمات السيبرانية، وبيان مدى كفايته وفاعليته في تحقيق متطلبات الأمن القومي وضمان حماية المرفق العام واستمراريته، ويتفرع عن هذا الهدف الرئيس مجموعة من الأهداف، تتمثل في الآتي:

1. بيان الإطار المفاهيمي والقانوني للأموال العامة والهجمات السيبرانية، وتحديد طبيعة المخاطر التي تتعرض لها الأموال العامة في البيئة الرقمية.
2. تحديد الأساس القانوني لحماية الأموال العامة من الاعتداءات السيبرانية، وبيان مدى استيعاب القواعد التقليدية لحماية المال العام للصور المستحدثة من الاعتداء الإلكتروني.
3. تحليل التشريعات الليبية المنظمة لحماية الأموال العامة ومكافحة الجرائم الإلكترونية، وبيان مدى كفايتها في مواجهة الهجمات التي تستهدف الأنظمة والبيانات والأموال التابعة للجهات العامة.
4. بيان العلاقة بين حماية الأموال العامة والأمن القومي، وتحديد الحالات التي يمكن فيها أن يرتقي الهجوم السيبراني على الأموال أو الأنظمة العامة إلى مستوى التهديد للأمن الاقتصادي أو السيبراني أو القومي للدولة.
5. تحليل أثر الهجمات السيبرانية على المرافق العامة، ولا سيما من حيث قدرتها على الانتظام والاستمرار في تقديم خدماتها وعدم تعطيلها نتيجة الاعتداء على أنظمتها الرقمية.
6. تحديد المسؤوليات القانونية والإدارية المترتبة على الجهات العامة في مجال تأمين الأنظمة والبيانات والأموال التي تديرها إلكترونياً، وبيان حدود المسؤولية الناشئة عن الإخلال بمتطلبات الحماية السيبرانية.
7. الكشف عن أوجه القصور أو الفراغ التشريعي والمؤسسي في النظام القانوني القائم فيما يتعلق بحماية الأموال العامة من الهجمات السيبرانية.
8. الاستفادة من بعض التجارب والتشريعات المقارنة في مجال الأمن السيبراني وحماية البنية التحتية والمرافق العامة، بما يمكن أن يساهم في تطوير التنظيم القانوني الليبي.
9. اقتراح مجموعة من الآليات والحلول التشريعية والمؤسسية التي تساهم في بناء منظومة قانونية متكاملة لحماية الأموال العامة من الهجمات السيبرانية، تجمع بين الوقاية والاستجابة والمساءلة وضمان استمرارية المرافق العامة.

ثانياً: أهمية الدراسة:

تتبع أهمية هذه الدراسة من حادثة موضوعها وتزايد المخاطر السيبرانية المرتبطة بالتحول الرقمي للمؤسسات والمرافق العامة، فضلاً عن اتصال حماية الأموال العامة بصورة مباشرة بالمصلحة العامة والأمن الاقتصادي واستمرارية الخدمات التي تقدمها الدولة. ويمكن بيان أهمية الدراسة من خلال جانبين رئيسيين:

1. الأهمية العلمية:

تتمثل الأهمية العلمية للدراسة في تناولها موضوعاً يقع عند نقطة الالتقاء بين القانون الإداري، وحماية الأموال العامة، والقانون الجنائي، والأمن السيبراني، والأمن القومي، وهو ما يمنحها طبيعة قانونية متعددة الأبعاد. كما تساهم الدراسة في توضيح التطور الذي طرأ على مفهوم حماية المال العام في ظل البيئة الرقمية؛ إذ لم تعد الحماية تقتصر على مواجهة الاختلاس أو الاستيلاء أو الإتلاف المادي، وإنما أصبحت تشمل حماية الأنظمة الإلكترونية وقواعد البيانات والمنصات التي يتم من خلالها إدارة الأموال العامة. وتبرز أهميتها كذلك في محاولة تأصيل العلاقة القانونية بين الهجمات السيبرانية ومبدأ استمرارية المرفق العام، وبيان مدى اعتبار الأمن الرقمي للجهات العامة أحد المتطلبات الحديثة لضمان انتظام المرافق العامة واستمرارها. كما تساهم الدراسة في إثراء الدراسات القانونية الليبية المتعلقة بالأمن السيبراني، من خلال الربط بين حماية المال العام والأمن القومي والمرفق العام ضمن إطار تحليلي واحد، والكشف عن المسائل القانونية المستحدثة التي قد لا تستوعبها بصورة كاملة القواعد التقليدية لحماية الأموال العامة.

2. الأهمية العملية:

تتمثل الأهمية العملية للدراسة في إمكانية الاستفادة من نتائجها في تقييم كفاية التشريعات الليبية القائمة ومدى قدرتها على مواجهة الاعتداءات السيبرانية التي تستهدف الأموال والأنظمة التابعة للدولة والمرافق العامة. كما يمكن أن تساهم الدراسة في تحديد مواطن القصور في توزيع الاختصاصات والمسؤوليات بين الجهات المعنية بحماية الأموال العامة والأمن السيبراني، بما يساعد على تعزيز التنسيق المؤسسي بين الجهات الإدارية والرقابية والأمنية والقضائية والفنية.

وتكتسب الدراسة أهمية خاصة بالنسبة إلى المرافق العامة الحيوية التي تعتمد بصورة متزايدة على النظم الإلكترونية في إدارة الأموال والبيانات وتقديم الخدمات، مثل قطاعات المالية والمصارف والطاقة والنفط والاتصالات وغيرها، لما قد يترتب على تعطيل أنظمتها من آثار مالية وإدارية وأمنية تتجاوز المرفق المستهدف إلى مصالح الدولة والمجتمع. وأخيراً، يمكن أن توفر النتائج والتوصيات التي تنتهي إليها الدراسة أساساً لتطوير السياسة التشريعية الليبية في مجال الأمن السيبراني وحماية الأموال العامة، بما يساهم في تعزيز الحماية الوقائية، ورفع كفاءة الاستجابة للحوادث السيبرانية، وتحديد المسؤوليات، وضمان استمرارية المرافق العامة، وتعزيز قدرة الدولة على حماية مصالحها وأمنها القومي في البيئة الرقمية.

تقسيم الإطار النظري إلى أربعة محاور رئيسية:

المحور الأول: الإطار المفاهيمي والقانوني للأموال العامة:

تحتل الأموال العامة مكانة أساسية في البناء القانوني للدولة، بالنظر إلى ارتباطها المباشر بأداء الوظائف العامة وتحقيق المصالح الجماعية وتمكين المرافق العامة من الاستمرار في تقديم خدماتها. فالمال العام لا يمثل مجرد قيمة مالية تدخل ضمن الذمة المالية للدولة أو أحد الأشخاص الاعتبارية العامة، وإنما يعد وسيلة ضرورية لممارسة النشاط الإداري والاقتصادي والاجتماعي وتحقيق الأهداف التي تضطلع بها السلطات العامة. ومن ثم، ارتبطت الحماية القانونية للأموال العامة بحماية المصلحة العامة ذاتها، وأحاطتها التشريعات بقواعد تختلف في طبيعتها ونطاقها عن تلك التي تحكم الأموال المملوكة للأفراد (الغزير، 2017، ص ص 261-265).

ويكتسب تحديد مفهوم المال العام أهمية خاصة في موضوع هذه الدراسة؛ إذ إن تحديد نطاق الأموال التي تتمتع بصفة العمومية يمثل نقطة البداية لتحديد نطاق الحماية القانونية المقررة لها، ومدى إمكانية امتداد هذه الحماية إلى الأموال والحقوق والبيانات والأنظمة الرقمية المرتبطة بإدارة الموارد العامة. وقد أظهر المشرع الليبي اهتماماً واضحاً بحماية المال العام من خلال القانون المدني والتشريعات الجنائية والاقتصادية، كما أكد القضاء الليبي أن اكتساب المال صفة العمومية يرتبط أساساً بتخصيصه للمنفعة العامة.

أولاً: مفهوم الأموال العامة:

يعد التمييز بين الأموال العامة والأموال الخاصة للدولة من الموضوعات الأساسية في القانون الإداري؛ فالدولة والأشخاص الاعتبارية العامة قد تمتلك أموالاً تخضع للقواعد المقررة للأموال العامة، كما قد تمتلك أموالاً أخرى تخضع – من حيث الأصل – لقواعد القانون الخاص. ولذلك لا يكفي أن يكون المال مملوكاً للدولة حتى يكتسب تلقائياً صفة المال العام، وإنما يتطلب الأمر توافر الشروط التي حددها القانون لاكتساب هذه الصفة.

ويُعرّف المال العام في الفقه الإداري بأنه المال المملوك للدولة أو لأحد الأشخاص الاعتبارية العامة والمخصص لتحقيق منفعة عامة، سواء تم هذا التخصيص بطبيعته واستعماله الفعلي أم بمقتضى أداة قانونية صادرة عن السلطة المختصة. ومن هذا المنطلق، يقوم مفهوم المال العام على عنصرين أساسيين هما ملكية شخص عام للمال وتخصيصه للمنفعة العامة.

وقد تبنى المشرع الليبي هذا الاتجاه بصورة واضحة في المادة (1/87) من القانون المدني الليبي، التي تعتبر من الأموال العامة العقارات والمنقولات المملوكة للدولة أو للأشخاص الاعتبارية العامة متى كانت مخصصة للمنفعة العامة بالفعل أو بمقتضى قانون أو قرار صادر عن السلطة المختصة. ومن ثم، فإن النص الليبي لم يكتف بعنصر الملكية العامة، وإنما اشترط إلى جانبه وجود تخصيص للمنفعة العامة.

ويؤكد ذلك أن صفة العمومية ليست ملازمة لكل ما تملكه الدولة، وإنما تكتسب بسبب الوظيفة التي يؤديها المال والغرض الذي خصص لتحقيقه. ولهذا تشير الدراسات الليبية إلى أن النظام القانوني للمال العام يرتبط بصورة جوهرية بقاعدة التخصيص للمنفعة العامة، وأن الحماية الاستثنائية المقررة لهذه الأموال تستهدف في النهاية حماية النشاط العام الذي خصص المال لخدمته (الغزير، 2017، ص ص 261-295).

ثانياً: معايير تمييز المال العام عن المال الخاص:

مر تحديد الأموال العامة بعدة اتجاهات فقهية، حاول كل منها وضع معيار يسمح بتمييزها عن الأموال الخاصة التي تملكها الدولة.

1. **معيار طبيعة المال:** ذهب اتجاه تقليدي إلى ربط صفة العمومية بطبيعة المال ذاته، بحيث تعد من الأموال العامة الأشياء التي تكون بطبيعتها معدة للاستعمال الجماعي، كالطرق والجسور والساحات العامة والموانئ. إلا أن هذا المعيار تعرض للنقد؛ لأن طبيعة المال وحدها لا تكفي لتحديد نظامه القانوني، فقد يكون الشيء صالحاً للاستخدام العام ولكنه غير مخصص له، كما يمكن تخصيص أموال لا تتميز بطبيعة خاصة لخدمة مرفق أو منفعة عامة.

2. **معيار تخصيص المال للاستعمال المباشر للجمهور:** وفقاً لهذا الاتجاه، يعد المال عامّاً إذا خصص لاستعمال الجمهور مباشرة، كالطرق والحدائق والساحات والشواطئ العامة. ويتميز هذا المعيار بربطه صفة المال العام بالغرض الاجتماعي الذي يؤديه، إلا أنه لا يستوعب جميع الأموال العامة، وبصفة خاصة الأموال التي لا يستعملها الجمهور مباشرة وإنما تخصص لخدمة مرفق عام.

3. **معيار تخصيص المال للمرفق العام:** اتجه جانب من الفقه إلى اعتبار المال عامّاً متى كان مخصصاً لمرفق عام وكان ضرورياً أو معدّاً بصورة خاصة لخدمة هذا المرفق. وتبرز أهمية هذا المعيار بالنسبة إلى الدراسة الحالية؛ لأن الأموال والأنظمة التقنية والمعلوماتية التي تستخدمها المرافق العامة الحديثة قد لا تكون معدة للاستعمال المباشر للجمهور، ولكنها قد تمثل عناصر أساسية في تشغيل المرفق واستمراره.

4. **معيار التخصيص للمنفعة العامة:** يعد هذا المعيار أوسع المعايير وأكثرها ملاءمة للتشريع الليبي؛ لأنه لا يحصر المال العام في الأشياء المستعملة مباشرة من الجمهور أو المخصصة لمرفق بعينه، وإنما يركز على تخصيص المال لتحقيق المنفعة العامة. وقد أخذ القانون المدني الليبي بهذا المعيار صراحة في المادة (87).

ويؤيد القضاء الليبي هذا الاتجاه؛ فقد قررت المحكمة العليا الليبية في الطعن الإداري رقم (62/43 ق)، الصادر في 23 يناير 2000، أن عقارات الدولة أو الأشخاص الاعتبارية العامة تصبح أموالاً عامة بمجرد تخصيصها للمنفعة العامة بقرار صادر عن الجهة المختصة، في حين أن عقارات الأفراد لا تكتسب هذه الصفة بمجرد صدور قرار نزع الملكية،

وإنما يلزم الاستيلاء عليها وضمها فعلياً إلى المال العام. ويؤكد هذا الحكم أهمية عنصر التخصيص الفعلي أو القانوني في تحديد صفة المال العام.

ثالثاً: عناصر اكتساب المال صفة العمومية:

يمكن في ضوء المادة (87) من القانون المدني الليبي والاتجاه القضائي استخلاص عنصرين رئيسيين لاكتساب المال صفة العمومية:

1. ملكية المال للدولة أو لشخص اعتباري عام:
يشترط ابتداءً أن يكون المال مملوكاً للدولة أو لأحد الأشخاص الاعتبارية العامة. ويشمل ذلك الأموال التابعة للوزارات والبلديات والهيئات والمؤسسات العامة وغيرها من الأشخاص الاعتبارية العامة في الحدود التي يحددها القانون. إلا أن المفهوم الجنائي للمال العام قد يكون أوسع نطاقاً من المفهوم المدني؛ فقد توسع المشرع الليبي في تحديد الأموال التي تتمتع بالحماية الجنائية. إذ نصت المادة (3) من القانون رقم (2) لسنة 1979 بشأن الجرائم الاقتصادية على اعتبار الأموال المملوكة أو الخاضعة لإدارة أو إشراف الجهات المحددة في القانون، أو أي جهة أخرى ينص القانون على اعتبار أموالها عامة، من الأموال العامة لأغراض تطبيق أحكام ذلك القانون. ويكشف ذلك عن اختلاف وظيفي مهم؛ فالقانون المدني يحدد المال العام أساساً انطلاقاً من الملكية والتخصيص للمنفعة العامة، بينما يتجه التشريع الجنائي الاقتصادي إلى توسيع نطاق الحماية ليشمل أموالاً تخضع لإدارة أو إشراف جهات عامة، ولو اقتضت الحماية الجنائية التعامل معها بمفهوم أوسع للمال العام.
2. تخصيص المال للمنفعة العامة:

يمثل التخصيص العنصر الجوهري الثاني. وقد يكون التخصيص فعلياً عندما تستخدم الجهة العامة المال بصورة فعلية لتحقيق منفعة عامة، وقد يكون قانونياً عندما يصدر قانون أو قرار من السلطة المختصة بتخصيصه لهذا الغرض. ويترتب على ذلك أن المال قد يكون مملوكاً للدولة دون أن يكون مالاً عاماً بالمعنى الفني، فإذا لم يكن مخصصاً للمنفعة العامة فإنه يدخل – من حيث الأصل – ضمن أموال الدولة الخاصة. ولذلك تعد فكرة التخصيص الحد الفاصل بين النظام القانوني الاستثنائي للأموال العامة والنظام الذي يحكم أموال الدولة الخاصة.

رابعاً: أنواع الأموال العامة:

تتنوع الأموال العامة تبعاً لطبيعتها والغرض الذي خصصت من أجله، ويمكن تقسيمها إلى عدة صور. فمن حيث طبيعة المال، توجد الأموال العامة العقارية، مثل الأراضي والمباني والمنشآت العامة والطرق والموانئ والمطارات، والأموال العامة المنقولة، مثل المعدات والآلات ووسائل النقل والأجهزة المخصصة لخدمة الجهات والمرافق العامة. ومن حيث طريقة الانتفاع بها، يمكن التمييز بين الأموال المخصصة للاستعمال المباشر للجمهور، كالطرق والساحات العامة، وبين الأموال المخصصة لخدمة المرافق العامة، كالمباني والأجهزة والمعدات والوسائل اللازمة لتشغيل المرفق. كما يمكن الحديث، في ضوء التحول الرقمي، عن أصول ذات طبيعة غير مادية تتصل اتصالاً مباشراً بالنشاط المالي والإداري للدولة، مثل قواعد البيانات والسجلات الإلكترونية والبرمجيات والمنصات الحكومية وأنظمة الدفع والتحصيل والحسابات الرقمية. وهنا تظهر إحدى القضايا القانونية الرئيسية التي سنتناولها الدراسة، وهي مدى إمكانية إخضاع هذه الأصول للحماية القانونية ذاتها أو لحماية مماثلة متى كانت ضرورية لإدارة المال العام أو تشغيل المرفق العام.

خامساً: خصائص الأموال العامة:

تتميز الأموال العامة بنظام قانوني استثنائي يستهدف ضمان استمرار تخصيصها للمنفعة العامة ومنع إخراجها من وظيفتها نتيجة تصرفات الأفراد أو الجهات الإدارية. وقد حددت المادة (87/2) من القانون المدني الليبي أهم مظاهر هذه الحماية بنصها على عدم جواز التصرف في الأموال العامة أو الحجز عليها أو تملكها بالتقادم.

1. عدم جواز التصرف في المال العام:

الأصل أن المال العام لا يجوز التصرف فيه بما يتعارض مع تخصيصه للمنفعة العامة. والغرض من هذا القيد ليس تجريد الإدارة من جميع سلطاتها على المال، وإنما المحافظة على تخصيصه ومنع نقله إلى الملكية الخاصة بطريقة تؤدي إلى تعطيل المنفعة العامة التي خصص لتحقيقها.

ويترتب على ذلك أن إخراج المال من نطاق الأموال العامة يستلزم أولاً إنهاء تخصيصه للمنفعة العامة، ثم يصبح بعد ذلك من الأموال الخاصة للدولة، ويجوز التصرف فيه وفقاً للقواعد القانونية المنظمة لذلك.

2. عدم جواز الحجز على الأموال العامة:

قرر المشرع عدم جواز الحجز على المال العام، لأن الحجز تمهيداً للتنفيذ الجبري والبيع يتعارض مع تخصيص المال للمنفعة العامة، كما يمكن أن يؤدي إلى تعطيل المرفق العام الذي يعتمد عليه.

وتظهر أهمية هذه القاعدة في أنها لا تستهدف فقط حماية ملكية الدولة، وإنما تستهدف بصورة أعمق حماية استمرارية النشاط العام. ومن هنا تبرز الصلة بين النظام القانوني للمال العام ومبدأ استمرار المرفق العام، وهي صلة ستصبح أكثر أهمية عند تناول الهجمات السيبرانية التي يمكن أن تؤدي إلى تعطيل الأموال والأنظمة الرقمية للمرافق العامة.

3. عدم جواز اكتساب المال العام بالتقادم:

لا يجوز للأفراد اكتساب ملكية المال العام عن طريق وضع اليد عليه مهما طالّت مدة الحيازة، طالما بقي المال محتفظاً بصفته العامة. وهذه الحماية مقررة بسبب استمرار تخصيص المال للمنفعة العامة، ومن ثم لا يمكن للحيازة الفردية أن تؤدي إلى إخراجها من نطاق المال العام.

وقد أشارت دراسة الغزير إلى أن الحماية المدنية التي أقرها المشرع الليبي تركز بصورة أساسية على القيود الثلاثة الواردة بالمادة (87)، وأن القضاء الليبي تعامل معها بوصفها أحكاماً مرتبطة بثبوت صفة المال العام (الغزير، 2017، ص ص 261-295).

سادساً: فقدان المال لصفة العمومية:

صفة المال العام ليست أبدية، وإنما تستمر ما دام المال مخصصاً للمنفعة العامة. وقد نظمت المادة (88) من القانون المدني الليبي هذه المسألة، مقررة أن المال يفقد صفته العامة بانتهاء تخصيصه للمنفعة العامة، وأن انتهاء التخصيص يمكن أن يتم بمقتضى أداة قانونية، أو بالفعل، أو بانتهاء الغرض الذي خصص المال من أجله.

وبالتالي، فإن انتهاء صفة العمومية يرتبط بانتهاء العنصر الذي منح المال هذه الصفة ابتداءً، وهو التخصيص للمنفعة العامة. فإذا انتهى التخصيص، أصبح المال - من حيث الأصل - من الأموال الخاصة للدولة، وأمكن إخضاعه للنظام القانوني المقرر لهذه الأموال.

سابعاً: الحماية القانونية للأموال العامة في التشريع الليبي:

لم يكثف المشرع الليبي بالحماية المدنية للأموال العامة، وإنما دعمها بحماية جنائية تستهدف مواجهة الأفعال التي تؤدي إلى الاعتداء عليها أو الإضرار بها. ويبرز في هذا المجال القانون رقم (2) لسنة 1979 بشأن الجرائم الاقتصادية، الذي استهل أحكامه بتقرير أن للأموال العامة حرمة وأن حمايتها واجب، ثم وضع مفهوماً واسعاً للمال العام لأغراض الحماية الجنائية.

وقد جرم القانون صوراً متعددة للاعتداء على المال والمصلحة العامة. فالمادة (9) تعاقب على إحداث ضرر جسيم عمداً بمال عام أو مصلحة عامة، بينما تناولت المادة (10) مسؤولية الموظف العام عندما يتسبب بخطفه الجسيم في هذا الضرر نتيجة الإهمال في أداء الوظيفة أو الإخلال بواجباتها أو إساءة استعمال السلطة.

وتكتسب هاتان المادتان أهمية خاصة بالنسبة إلى موضوع الدراسة؛ لأن حماية المال العام من المخاطر السيبرانية لا تثير فقط مسؤولية الشخص الذي ينفذ الهجوم عمداً، وإنما يمكن أن تثير أيضاً - بحسب الوقائع والنصوص الواجبة التطبيق - مسألة المسؤولية عن الإهمال الجسيم في حماية الأنظمة والأصول العامة إذا أدى إلى وقوع ضرر بالمال العام.

كما تنص المادة (15) من القانون ذاته على معاقبة الموظف العام المكلف بحفظ أو صيانة مال عام إذا قصر في حفظه أو صيانته، مع إمكان إلزامه بقيمة الأضرار التي تلحق بالمال العام نتيجة تقصيره.

ويطرح هذا النص تساؤلاً مهماً في البيئة الرقمية: هل يمكن أن يمتد مفهوم واجب الحفظ والصيانة إلى تأمين الأنظمة الرقمية وقواعد البيانات والحسابات والمنصات التي تدار من خلالها الأموال العامة؟ فهذه الأنظمة قد أصبحت في الإدارة الحديثة من الوسائل الأساسية لحفظ المال العام وإدارته ومراقبته، وبالتالي فإن التقصير في أمنها السيبراني يمكن أن يؤدي عملياً إلى نتائج لا تقل خطورة عن التقصير في حماية المال المادي ذاته.

كذلك جرم القانون اختلاس المال العام والاستيلاء عليه دون وجه حق؛ فنصت المادة (27) على معاقبة الموظف العام الذي يختلس أموالاً عامة أو أموالاً مسلمة إليه بحكم وظيفته، بينما تعاقب المادة (28) الموظف العام الذي يستولي دون وجه حق على مال عام.

ويؤكد هذا التنظيم أن السياسة التشريعية الليبية أقامت حماية جنائية واسعة للأموال العامة تشمل التخريب والإضرار والاختلاس والاستيلاء والتقصير في الحفظ والصيانة، إلا أن معظم هذه الأحكام نشأت في سياق المال بصورته التقليدية، الأمر الذي يثير الحاجة إلى بحث مدى قدرتها على استيعاب الاعتداءات التي تقع بواسطة التقنيات الرقمية.

ثامناً: الأموال العامة في ظل التحول الرقمي:

أدى التحول الرقمي في الإدارة العامة إلى تغير جوهري في الطريقة التي تُدار بها الأموال العامة؛ فلم تعد العمليات المتعلقة بالمال العام تعتمد على المستندات الورقية والتعاملات المادية فقط، وإنما أصبحت تتم عبر أنظمة وقواعد بيانات وشبكات ومنصات إلكترونية.

وتشمل هذه البيئة أنظمة صرف المرتبات، والتحويل الإلكتروني للإيرادات العامة، وأنظمة الموازنة والحسابات الحكومية، والسجلات الضريبية والجمركية، وأنظمة المشتريات والعقود الحكومية، والحسابات المصرفية التابعة للجهات العامة، وغيرها من الأدوات الرقمية التي أصبحت جزءاً من إدارة الموارد العامة. ويقتضي ذلك التمييز بين المال العام ذاته وبين البنية الرقمية المرتبطة بإدارته. فقاعدة البيانات أو النظام الإلكتروني لا يصبح بالضرورة مالاً عامّاً بالمعنى التقليدي لمجرد اتصاله بجهة عامة، إلا أن الاعتداء عليه قد يؤدي بصورة مباشرة إلى الاستيلاء على المال العام أو تعطيله أو تغيير قيمته أو حرمان المرفق العام من الانتفاع به. ومن ثم، لم تعد الحماية الفعالة للمال العام ممكنة من خلال حماية المال في صورته المادية فقط، وإنما ينبغي أن تمتد إلى سلامة البيانات والأنظمة والشبكات التي تتيح حيازته وإدارته والتصرف فيه ومراقبته.

وتتضح هنا الحاجة إلى تطوير مفهوم الحماية القانونية من فكرة حماية الشيء العام إلى حماية المنظومة التي تدير المال العام؛ لأن اختراق نظام إلكتروني مالي تابع للدولة قد يسمح للمعتدي بتحويل الأموال أو تغيير البيانات أو إخفاء المعاملات أو تعطيل الوصول إلى الموارد المالية، دون أن يقع اعتداء مادي مباشر على شيء ملموس.

تاسعاً: نحو مفهوم وظيفي للمال العام في البيئة الرقمية:

تدفع التطورات التقنية نحو ضرورة النظر إلى المال العام من منظور وظيفي لا يقتصر على طبيعته المادية، وإنما يأخذ في الاعتبار القيمة والمصلحة والوظيفة العامة التي يحميها القانون.

وإذا كان معيار التخصيص للمنفعة العامة يمثل الأساس الذي يقوم عليه مفهوم المال العام في المادة (87) من القانون المدني الليبي، فإن هذا المعيار يمكن أن يشكل نقطة انطلاق مهمة لدراسة الأصول الرقمية المخصصة بصورة كاملة لخدمة المرافق العامة أو لإدارة الموارد العامة، مع ضرورة التمييز بين التفسير القضائي للنص القائم وبين أي توسع تشريعي مستقبلي مطلوب.

ولا ينبغي افتراض أن جميع البيانات والبرمجيات والمنصات الحكومية تدخل تلقائياً ضمن تعريف المال العام الوارد في المادة (87)، لأن النص يتحدث عن العقارات والمنقولات. إلا أن التحول الرقمي يطرح حاجة تشريعية إلى تحديد المركز القانوني للأصول الرقمية العامة بصورة أكثر وضوحاً، خاصة عندما يؤدي الاعتداء عليها إلى إهدار المال العام أو تعطيل مرفق حيوي أو تهديد مصلحة قومية.

ومن ثم، يمكن القول إن الحماية الحديثة للأموال العامة ذات طبيعة مزدوجة: حماية مباشرة للمال العام من الاختلاس والاستيلاء والإتلاف والإهدار، وحماية غير مباشرة للبنية الرقمية التي يتم من خلالها حفظ المال وإدارته وتحويله ومراقبته. وهذا الامتداد هو الذي يربط التأصيل التقليدي للمال العام بموضوع الدراسة الحالي المتعلق بالهجمات السيبرانية. يتبين مما سبق أن النظام القانوني الليبي يقوم في تحديد المال العام على عنصرين رئيسيين هما ملكية الدولة أو الشخص الاعتباري العام، والتخصيص للمنفعة العامة، وأن المشرع أحاط هذه الأموال بنظام حماية خاص يقوم مدنياً على عدم جواز التصرف فيها أو الحجز عليها أو تملكها بالتقادم، وجنائياً على تجريم صور متعددة من الاعتداء عليها، بما فيها الإضرار والاختلاس والاستيلاء والتقصير في الحفظ والصيانة. كما أكد القضاء الليبي الدور الحاسم للتخصيص للمنفعة العامة في اكتساب المال صفة العمومية.

غير أن التحول الرقمي يثير تحدياً جديداً يتمثل في أن إدارة الأموال العامة أصبحت مرتبطة بأنظمة وبيانات ومنصات رقمية قد تكون هي ذاتها محلاً للهجوم، وهو ما يستدعي تجاوز التصور التقليدي للحماية إلى تصور أشمل يربط حماية المال العام بحماية بنيته الرقمية. ومن هنا ينتقل البحث إلى المحور الثاني لدراسة طبيعة الهجمات السيبرانية وصورها ومدى ما تمثله من مخاطر على الأموال العامة.

المحور الثاني: الهجمات السيبرانية ومخاطرها على الأموال العامة:

أدى التطور المتسارع في تقنيات المعلومات والاتصالات إلى تغير طبيعة المخاطر التي تواجه الدولة ومؤسساتها؛ فبعد أن كانت الاعتداءات على الأموال والمصالح العامة ترتبط في الغالب بأفعال مادية مباشرة، أصبح من الممكن ارتكاب اعتداءات واسعة النطاق من خلال الفضاء السيبراني، بما يسمح بالوصول غير المشروع إلى الأنظمة وقواعد البيانات، والتلاعب بالمعلومات، وتعطيل الخدمات، وتحويل الأموال، والاستيلاء على بيانات التعريف، وإخفاء الأدلة الرقمية. وقد ترتب على ذلك أن أصبحت الهجمات السيبرانية أحد التحديات القانونية والأمنية الرئيسية التي تواجه المؤسسات العامة في العصر الرقمي.

وتزداد أهمية هذه المخاطر مع اعتماد الجهات العامة على الأنظمة الإلكترونية في إدارة مواردها المالية وتنفيذ معاملاتها وحفظ سجلاتها؛ إذ يمكن أن يؤدي اختراق نظام معلوماتي تابع لجهة عامة إلى آثار مالية لا تقل خطورة عن الاعتداء المادي المباشر على المال العام. وقد أكدت دراسات ليبية حديثة أن المؤسسات الليبية تعرضت لصور من التهديدات السيبرانية، بما في ذلك مؤسسات اقتصادية واستراتيجية، وأن الآثار المترتبة على تلك التهديدات يمكن أن تمتد إلى الأمن القومي والاستقرار المؤسسي (حامد، 2023، ص 256-280؛ عصمان، 2025).

ومن هنا تبرز ضرورة تحديد ماهية الهجمات السيبرانية وخصائصها وصورها، والتمييز بينها وبين الجريمة الإلكترونية، ثم تحليل كيفية تحول المال العام والأنظمة المرتبطة بإدارته إلى أهداف محتملة لهذه الهجمات، وصولاً إلى تحديد الآثار القانونية والمالية والإدارية التي يمكن أن تترتب عليها.

أولاً: مفهوم الفضاء السيبراني:

يمثل الفضاء السيبراني البيئة الرقمية التي تنشأ من خلال ترابط أنظمة المعلومات والحواسيب والشبكات وقواعد البيانات والبرمجيات ووسائل الاتصال، والتي تتم عبرها عمليات إنشاء المعلومات وتخزينها ومعالجتها ونقلها وتبادلها. ولم يعد هذا الفضاء منفصلاً عن النشاط الواقعي للدولة؛ إذ أصبحت المؤسسات العامة تعتمد عليه في إدارة جانب كبير من أعمالها وخدماتها ومواردها.

ويترتب على ذلك أن الفضاء السيبراني أصبح مجالاً جديداً لممارسة السلطة والنشاط الاقتصادي والإداري، وفي الوقت نفسه مجالاً لظهور مخاطر وتهديدات يمكن أن تصيب الدولة والأفراد والمؤسسات. ويرى العمري أن اتساع الاعتماد على الأنظمة والشبكات الرقمية جعل الأمن السيبراني عنصراً ضرورياً لحماية المعلومات والأنظمة من الدخول أو الاستخدام أو التعديل أو التعطيل غير المشروع (العمري، 2020).

وفي السياق الليبي، تظهر أهمية هذا المجال بصورة متزايدة نتيجة توسع الاعتماد على قواعد البيانات والأنظمة الإلكترونية في المؤسسات العامة. وقد أكدت دراسة عقيل أن قواعد البيانات السيادية يمكن أن تتحول إلى هدف لتهديدات رقمية تؤثر في مصالح الدولة، وأن ضعف الحوكمة والحماية التقنية والتشريعية يزيد من خطورة هذه التهديدات (عقيل، 2026، ص ص 66-82).

ثانياً: مفهوم الأمن السيبراني:

يقصد بالأمن السيبراني مجموعة التدابير القانونية والتنظيمية والتقنية والبشرية التي تستهدف حماية الأنظمة والشبكات والبرامج والبيانات من الاختراق أو الاستخدام غير المشروع أو الإتلاف أو التعديل أو التعطيل، وضمان قدرة هذه الأنظمة على أداء وظائفها بصورة آمنة ومستقرة.

ولا ينبغي حصر الأمن السيبراني في الوسائل التقنية؛ فهو يقوم على مجموعة متكاملة من العناصر تشمل التشريع، وإدارة المخاطر، والحوكمة، وحماية البيانات، والرقابة، والاستجابة للحوادث، والتعافي، والتوعية والتدريب. ولذلك أصبح الأمن السيبراني قضية قانونية ومؤسسية إلى جانب كونه قضية تقنية.

وقد انعكس هذا التصور في التطور المؤسسي الليبي؛ إذ نص قرار مجلس الوزراء رقم (358) لسنة 2026 بشأن إنشاء الهيئة الوطنية للأمن السيبراني والسيادة الرقمية على أن من أهداف الهيئة وضع السياسات والاستراتيجيات والمعايير الوطنية للأمن السيبراني، وتأمين البنية التحتية المعلوماتية ومواجهة مخاطر الهجمات السيبرانية بما يحافظ على الأمن القومي واستقرار عمل مؤسسات الدولة.

وهذا التطور مهم بالنسبة إلى الدراسة؛ لأنه يبين أن المشرع والتنظيم الإداري الليبي لم يعودا يتعاملان مع الأمن السيبراني باعتباره مجرد حماية فنية لأجهزة الحاسوب، وإنما باعتباره عنصراً يتصل مباشرة باستقرار مؤسسات الدولة وحماية المصالح الوطنية.

ثالثاً: مفهوم الهجمات السيبرانية:

يمكن تعريف الهجوم السيبراني بأنه نشاط متعمد يستخدم وسائل تقنية أو رقمية لاستهداف نظام معلوماتي أو شبكة أو جهاز أو بيانات، بقصد الدخول إليها أو السيطرة عليها أو تعطيلها أو تغييرها أو إتلافها أو الاستفادة منها بطريقة غير مشروعة.

ولا يستخدم القانون الليبي رقم (5) لسنة 2022 مصطلح «الهجوم السيبراني» بوصفه وصفاً جامعاً لكل الأفعال، وإنما نظم صوراً متعددة للأفعال التي يمكن أن تدخل في نطاقه. فقد عرفت المادة الأولى الاختراق بأنه الوصول إلى وسيلة من وسائل تقنية المعلومات بطريقة غير مشروعة من خلال ثغرات في نظام الحماية، كما عرفت الجريمة الإلكترونية بأنها كل فعل يرتكب باستخدام أنظمة الحاسب أو شبكة المعلومات أو غيرها من وسائل تقنية المعلومات بالمخالفة لأحكام القانون. ومن ثم، فإن مفهوم الهجوم السيبراني في هذه الدراسة أوسع من مجرد الدخول غير المشروع؛ فقد يشمل الدخول والتخريب والتعديل والتشفير والتعطيل والاستيلاء على البيانات أو استخدامها للوصول إلى الأموال أو تعطيل الخدمات العامة.

رابعاً: التمييز بين الهجوم السيبراني والجريمة الإلكترونية:

رغم التقارب بين المفهومين، فإنه ينبغي التمييز بين الجريمة الإلكترونية والهجوم السيبراني.

- **فالجريمة الإلكترونية** مفهوم قانوني يرتبط بتوافر سلوك مجرم بنص قانوني، وبالتالي يخضع لمبدأ الشرعية الجنائية الذي يقضي بأنه لا جريمة ولا عقوبة إلا بنص. وقد عرّف القانون رقم (5) لسنة 2022 الجريمة الإلكترونية من خلال ارتباط الفعل باستخدام أنظمة الحاسب أو شبكات المعلومات أو وسائل تقنية المعلومات بالمخالفة لأحكام القانون.
- **أما الهجوم السيبراني** فهو وصف أوسع لطبيعة النشاط التقني الموجه ضد نظام أو شبكة أو بيانات، وقد تتعدد الأفعال المكونة له بحيث يشكل الهجوم الواحد عدة جرائم إلكترونية، مثل الدخول غير المشروع وإتلاف البيانات وتعطيل النظام والاستيلاء على وسائل التعريف.

وتبرز أهمية هذا التمييز في موضوع الدراسة؛ لأن تحليل المخاطر التي تتعرض لها الأموال العامة لا ينبغي أن يقتصر على الوصف الجنائي النهائي للفعل، وإنما يجب أن يشمل أيضاً طبيعة الهجوم ووسيلته والهدف منه وآثاره ومدى قدرته على تعطيل المرفق العام أو الإضرار بالمصلحة العامة.

خامساً: خصائص الهجمات السيبرانية:

تتميز الهجمات السيبرانية بعدد من الخصائص التي تجعل مواجهتها أكثر تعقيداً من العديد من صور الاعتداء التقليدية:

1. **الطابع التقني:** تعتمد الهجمات السيبرانية على تقنيات وبرمجيات وشبكات قد تكون شديدة التعقيد، وهو ما يتطلب خبرة فنية متخصصة لاكتشاف الهجوم وتحديد مصدره وتحليل آثاره والحفاظ على الأدلة المتعلقة به.
2. **السرعة:** يمكن تنفيذ الاعتداء خلال فترة زمنية قصيرة جداً، كما يمكن نقل البيانات أو تغييرها أو تعطيل أنظمة متعددة بصورة متزامنة، بما يجعل التدخل اللاحق وحده غير كافٍ ويوجب تعزيز الحماية الوقائية.
3. **إمكانية إخفاء هوية الفاعل:** يمكن للمهاجم استخدام وسائل تقنية متعددة لإخفاء هويته وموقعه الحقيقي، وهو ما يثير صعوبات في تحديد مرتكب الاعتداء وجمع الأدلة وإسناد المسؤولية إليه.
4. **تجاوز الحدود الجغرافية:** قد يكون النظام المستهدف موجوداً في ليبيا، بينما ينفذ الهجوم من دولة أخرى أو عبر خوادم موجودة في عدة دول. وقد راعى المشرع الليبي هذه الطبيعة؛ إذ قرر القانون رقم (5) لسنة 2022 سريان أحكامه

على الجرائم التي ترتكب خارج ليبيا إذا امتدت نتائجها وآثارها إلى داخلها، حتى في بعض الحالات التي لا يكون فيها الفعل معاقباً عليه في الدولة التي وقع فيها.

5. **تعدد الآثار:** قد يؤدي الهجوم الواحد إلى خسارة مالية وتسريب بيانات وتعطيل خدمة عامة والإضرار بالثقة في المؤسسة المستهدفة في الوقت نفسه. ومن ثم فإن تقييم خطورة الهجوم يجب ألا يعتمد على مقدار الخسارة المالية وحدها.

سادساً: أبرز صور الهجمات السيبرانية المهددة للأموال العامة:

1. **الدخول غير المشروع إلى الأنظمة:** يمثل الدخول غير المشروع نقطة البداية في كثير من الهجمات، ويقع عندما يتمكن المهاجم من تجاوز وسائل الحماية والوصول إلى النظام دون تصريح. وقد عالج المشرع الليبي هذه الصورة في **المادتين (11 و12)** من القانون رقم (5) لسنة 2022. وشدد العقوبة عندما يكون الدخول بقصد حذف البيانات أو إضافتها أو تدميرها أو إفشائها أو إتلافها أو حجبها أو تعديلها أو نقلها أو نسخها أو تعطيل نظام المعلومات، كما ترتفع العقوبة عندما يؤدي الفعل فعلياً إلى إعاقة النظام أو تعطيل الشبكة أو إفساد محتوياتها. وتكتسب هذه النصوص أهمية مباشرة لحماية المال العام عندما يكون النظام المخترق مسؤولاً عن إدارة حسابات عامة أو بيانات مالية أو عمليات تحصيل وإنفاق أو سجلات مالية حكومية.
2. **البرمجيات الخبيثة والفيروسات:** يمكن استخدام البرمجيات الخبيثة للوصول إلى الأنظمة أو مراقبتها أو تغيير بياناتها أو إتلافها. وتزداد خطورتها عندما تستهدف شبكة مترابطة داخل مؤسسة عامة؛ لأن الضرر قد ينتقل من جهاز واحد إلى أنظمة متعددة. وقد أدرج القانون الليبي ضمن تعريفاته ومجالات تجريمه عدداً من الأدوات والأفعال التقنية المرتبطة بالفيروسات وإعاقة الأنظمة والوصول غير المشروع، بما يوفر أساساً قانونياً لمواجهة صور متعددة من هذه الاعتداءات.
3. **هجمات الفدية:** تقوم هجمات الفدية غالباً على الوصول إلى الأنظمة وتشفير البيانات أو منع المؤسسة من الوصول إليها، ثم مطالبتها بدفع مبلغ مالي مقابل إعادة الوصول إليها. وخطورتها على المرفق العام مزدوجة؛ فهي قد تؤدي إلى **خسارة مالية مباشرة** إذا دفعت أموال، وإلى تعطيل الخدمة العامة إذا أصبحت الأنظمة غير متاحة. وقد تصبح آثارها أشد خطورة عندما تستهدف مرفقاً مالياً أو صحياً أو خدمياً أو إحدى البنى التحتية الحيوية.
4. **هجمات حجب الخدمة:** تستهدف هذه الهجمات إغراق النظام أو الخادم بعدد كبير من الطلبات بما يؤدي إلى إبطائه أو توقفه عن العمل. ولا يشترط فيها أن يستولي المهاجم على الأموال أو البيانات؛ فقد يكون هدفه الأساسي تعطيل النظام. وتظهر هنا أهمية الانتقال من مفهوم حماية المال العام إلى مفهوم حماية القدرة على الانتفاع به وإدارته؛ فتعطيل نظام التحصيل أو الدفع أو الرواتب أو المشتريات الحكومية قد يؤدي إلى تعطيل عمليات مالية عامة دون الاستيلاء المباشر على المال.
5. **التلاعب بالبيانات والسجلات المالية:** يمثل التلاعب بالبيانات إحدى أخطر صور الاعتداء السيبراني؛ فقد يتم تغيير الأرصدة أو أرقام الحسابات أو بيانات المستفيدين أو قيم المدفوعات أو المستحقات أو السجلات المتعلقة بالإيرادات والنفقات. وفي هذه الحالة لا يكون محل الاعتداء النقود في صورتها المباشرة بالضرورة، وإنما البيانات التي تحدد كيفية التصرف فيها. ولذلك يمكن أن يؤدي تغيير بضعة بيانات إلكترونية إلى نقل مبالغ مالية كبيرة أو إخفاء واقعة مالية أو إنشاء استحقاق غير مشروع.
6. **الاستيلاء على الهوية ووسائل التعريف الرقمية:** يمكن أن يستهدف الهجوم كلمات المرور أو بيانات المستخدمين أو وسائل المصادقة، ثم تستخدم للوصول إلى النظام وكان الفاعل مستخدم مشروع. وقد جرم القانون رقم (5) لسنة 2022 الاستيلاء على أدوات التعريف والهوية واستخدامها بصورة غير مشروعة، وهو ما يكتسب أهمية خاصة بالنسبة إلى الحسابات والصلاحيات الإلكترونية للموظفين المكلفين بإدارة الأموال والأنظمة العامة.
7. **الاعتداءات على وسائل الدفع الإلكتروني:** تزداد المخاطر مع توسع استخدام وسائل الدفع والتحصيل الإلكتروني. وقد عالج القانون الليبي صوراً من الاعتداء على البطاقات المصرفية والنقود الإلكترونية، ومنها تقليد البطاقة الإلكترونية أو استخدام البطاقة المسروقة أو المقلدة وتزوير النقود الإلكترونية واستعمالها. وتبرز أهمية هذه الأحكام بالنسبة إلى الدراسة عندما ترتبط وسائل الدفع بحسابات أو موارد أو معاملات مالية عامة.

سابعاً: الأموال العامة كهدف للهجمات السيبرانية:

يمكن أن تستهدف الهجمات السيبرانية المال العام بطريقتين رئيسيتين:

- **الأولى: الاعتداء المباشر،** ويقع عندما تستخدم الوسائل الإلكترونية للاستيلاء على الأموال العامة أو تحويلها أو الحصول عليها دون حق.
 - **أما الثانية: الاعتداء غير المباشر،** فيقع باستهداف النظام أو البيانات التي يتم من خلالها حفظ المال العام أو إدارته أو تحصيله أو صرفه أو مراقبته.
- وتعد الصورة الثانية أكثر تعقيداً من الناحية القانونية؛ لأن محل الهجوم المباشر قد يكون قاعدة بيانات أو برنامجاً أو حساب مستخدم، بينما تكون النتيجة النهائية إهدار مال عام أو تعطيل إمكانية الانتفاع به.
- ومن هنا يمكن القول إن الأمن السيبراني أصبح أحد أدوات حماية المال العام؛ لأن سلامة المال في البيئة الرقمية أصبحت تعتمد بدرجة كبيرة على سلامة النظام الذي يديره.

ثامناً: مخاطر الهجمات السيبرانية على المؤسسات العامة الليبية:

لا تمثل المخاطر السيبرانية بالنسبة إلى ليبيا مجرد احتمال نظري. فقد أشارت دراسة عصمان إلى تعرض مؤسسات ليبية لهجمات وتهديدات سيبرانية، ومن بينها مصرف ليبيا المركزي والمؤسسة الوطنية للنفط، وخلصت إلى أن هذه التهديدات يمكن أن تسبب خسائر مادية وتنعكس على الأمن القومي والاستقرار (عصمان، 2025). كما خلصت حامد إلى أن التهديدات السيبرانية أصبحت من التحديات التي تواجه الأمن القومي الليبي، وأن مواجهتها تتطلب آليات واستراتيجيات داخلية وتعاوناً خارجياً ومؤسسات متخصصة في حماية أمن المعلومات (حامد، 2023، ص ص 256-280). وتكشف هذه النتائج عن أن المؤسسات المالية والنفطية وغيرها من الجهات التي تدير موارد عامة أو أصولاً استراتيجية يمكن أن تمثل أهدافاً عالية القيمة، لأن نجاح الهجوم عليها قد يحقق للمهاجم أثراً اقتصادياً ومؤسسياً يفوق بكثير مجرد اختراق نظام تقني.

تاسعاً: الآثار المالية للهجمات السيبرانية:

يمكن أن تؤدي الهجمات إلى خسائر مالية مباشرة من خلال تحويل الأموال أو الاستيلاء عليها، كما يمكن أن تنشأ خسائر غير مباشرة نتيجة تكاليف إصلاح الأنظمة واستعادة البيانات وتعطل الخدمات والتحقيق في الحادث وتعزيز الحماية بعد وقوعه.

وقد يؤدي التلاعب بالسجلات إلى إخفاء الإيرادات أو تضخيم النفقات أو تغيير المستفيدين أو إنشاء معاملات وهمية، وهو ما يجعل المخاطر السيبرانية مرتبطة كذلك بمكافحة الفساد وحماية النزاهة المالية. ويؤكد القانون رقم (5) لسنة 2022 أهمية البعد الاقتصادي للحماية عندما جعل من أهدافه صراحة حماية الاقتصاد الوطني وحفظ الحقوق المترتبة على الاستخدام المشروع للتقنيات وتعزيز الثقة في المعاملات الإلكترونية.

عاشرًا: الآثار الإدارية والمرفقية:

قد يؤدي الهجوم إلى تعطيل الأنظمة التي يعتمد عليها المرفق في تقديم خدماته، ومن ثم يمتد أثره إلى المواطنين والجهات الأخرى المرتبطة به. وتتجلى هذه الخطورة عندما يعتمد المرفق بصورة كاملة على نظام إلكتروني، بحيث يؤدي تعطيله إلى توقف الخدمة أو تأخيرها. وفي هذه الحالة يصبح الهجوم السيبراني تهديداً ليس للمال أو البيانات فحسب، وإنما لمبدأ انتظام المرفق العام واستمراره.

وهذا يوضح الصلة المباشرة بين المحور الحالي والمحور الثالث؛ إذ إن حماية المرفق العام في العصر الرقمي لا يمكن فصلها عن حماية بنيته المعلوماتية.

الحادي عشر: الآثار على الأمن القومي:

قد يتجاوز الهجوم نطاق المؤسسة المستهدفة عندما يتعلق بمرفق حيوي أو مؤسسة مالية أو نفطية أو اتصالية أو بقاعدة بيانات سيادية. وفي هذه الحالات قد تتحول المخاطر من مشكلة تقنية أو مالية محدودة إلى تهديد للأمن القومي. وقد أكدت دراسة عصمان أن تأثير التهديدات السيبرانية في المؤسسات الليبية يمكن أن ينعكس على الأمن القومي، بينما ربطت دراسة عقيل حماية قواعد البيانات السيادية بحماية الهوية والأمن الوطني (عصمان، 2025؛ عقيل، 2026، ص ص 66-82).

كما جاء قرار إنشاء الهيئة الوطنية للأمن السيبراني والسيادة الرقمية لسنة 2026 ليؤكد هذا الارتباط بصورة تنظيمية واضحة، عندما ربط تأمين البنية التحتية المعلوماتية والتصدي للهجمات السيبرانية بالمحافظة على الأمن القومي واستقرار عمل مؤسسات الدولة.

الثاني عشر: تحديات الإثبات في الهجمات السيبرانية:

تتميز الجرائم السيبرانية بأن أدلتها غالباً ذات طبيعة رقمية، مثل سجلات الدخول وعناوين الاتصال والملفات الإلكترونية وبيانات الأجهزة والسجلات الزمنية. وقد تكون هذه الأدلة قابلة للتغيير أو الحذف بصورة أسرع من الأدلة التقليدية. ولذلك عرف القانون الليبي رقم (5) لسنة 2022 الدليل الجنائي الرقمي ونظم عدداً من المسائل المتصلة بالجرائم المعلوماتية، كما جرم إتلاف الأدلة القضائية المعلوماتية أو إخفاءها أو تعديلها أو محوها أو العبث بها. وتكتسب المحافظة على الدليل أهمية خاصة في جرائم الاعتداء على المال العام؛ لأنها ضرورية لإثبات مسار الدخول إلى النظام، وتحديد العمليات التي أجريت، وربطها بالمتهم، وتحديد مقدار الضرر المالي.

الثالث عشر: الطبيعة العابرة للحدود وإشكالية الاختصاص:

يمكن تنفيذ الهجوم من خارج إقليم الدولة، وقد تمر البيانات والأوامر عبر خوادم موجودة في أكثر من دولة، وهو ما يثير مشكلات تتعلق بالاختصاص القضائي وجمع الأدلة وتسليم المتهمين والتعاون الدولي.

وقد حاول المشرع الليبي مواجهة جانب من هذه الإشكالية من خلال توسيع نطاق سريان القانون رقم (5) لسنة 2022 ليشمل الجرائم التي تقع خارج ليبيا عندما تمتد نتائجها وأثارها إلى الداخل. غير أن النص على الاختصاص وحده لا يحل جميع المشكلات العملية؛ إذ تظل فعالية الملاحقة مرتبطة بوجود آليات للتعاون القضائي وتبادل الأدلة والمعلومات، خصوصاً عندما تكون البنية المستخدمة في الهجوم موزعة بين عدة دول.

الرابع عشر: الحاجة إلى الانتقال من الحماية اللاحقة إلى الحماية الوقائية:

تكشف طبيعة الهجمات السيبرانية أن التجريم والعقاب بعد وقوع الاعتداء لا يكفيان وحدهما لحماية الأموال العامة. فإذا أدى الهجوم إلى تحويل أموال أو إتلاف قاعدة بيانات أو تعطيل مرفق حيوي، فقد يصعب إصلاح جميع النتائج حتى مع اكتشاف الجاني ومعاقبته.

ومن ثم، ينبغي أن يقوم النظام القانوني الحديث على الحماية الوقائية إلى جانب الحماية الجنائية، من خلال فرض معايير للأمن السيبراني، وتحديد المسؤوليات، وتقييم المخاطر، وتحديث الأنظمة، وإدارة صلاحيات الوصول، والنسخ الاحتياطي، والإبلاغ عن الحوادث، ووضع خطط لاستمرارية الأعمال والتعافي.

ويعكس إنشاء الهيئة الوطنية للأمن السيبراني والسيادة الرقمية سنة 2026 اتجاهاً نحو تعزيز هذا الجانب الوقائي والمؤسسي؛ إذ تشمل أهدافها وضع السياسات والاستراتيجيات والمعايير الوطنية وتأمين البنية التحتية المعلوماتية ومواجهة التهديدات السيبرانية.

يتضح أن الهجمات السيبرانية تمثل صورة مستحدثة من صور المخاطر التي تواجه الأموال العامة، وأن خطورتها لا تقتصر على الاستيلاء المباشر على الأموال، بل تمتد إلى اختراق الأنظمة، والتلاعب بالسجلات، وتعطيل الخدمات، والاستيلاء على الهويات الرقمية، وإتلاف البيانات، بما قد يؤدي في النهاية إلى إهدار المال العام أو تعطيل المرفق أو المساس بمصلحة وطنية حيوية.

وقد وفر القانون الليبي رقم (5) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية أساساً مهماً لتجريم عدد من الأفعال المرتبطة بهذه الهجمات، وخاصة الدخول غير المشروع والتأثير في الأنظمة والاستيلاء على أدوات التعريف والاعتداءات المتعلقة بوسائل الدفع والأدلة الرقمية. إلا أن طبيعة المخاطر السيبرانية تؤكد أن الحماية الجنائية اللاحقة لا تكفي بمفردها، وإنما ينبغي أن تندمج معها قواعد الوقاية وإدارة المخاطر والاستجابة والتعافي واستمرارية المرافق العامة.

وبذلك تظهر العلاقة الوثيقة بين ثلاثة مستويات للحماية: حماية المال العام، وحماية المرفق العام من التعطيل، وحماية الأمن القومي من الآثار التي قد تترتب على استهداف المؤسسات والبنى التحتية الحيوية. وهذا الترابط يمثل الأساس للانتقال إلى المحور الثالث المتعلق بحماية الأموال العامة من الهجمات السيبرانية في ضوء متطلبات الأمن القومي وحماية المرفق العام.

المحور الثالث: حماية الأموال العامة من الهجمات السيبرانية في ضوء الأمن القومي والمرفق العام:

أصبحت حماية الأموال العامة من الهجمات السيبرانية مسألة تتجاوز نطاق الحماية المالية أو الجنائية التقليدية، لما قد يترتب على هذه الهجمات من آثار تمس قدرة الدولة على أداء وظائفها واستمرار مرافقها العامة والمحافظة على استقرارها الاقتصادي والمؤسسي. فالأنظمة الرقمية لم تعد مجرد وسائل مساعدة للعمل الإداري، وإنما أصبحت جزءاً من البنية الأساسية التي تعتمد عليها مؤسسات الدولة في إدارة الأموال والبيانات والخدمات، وهو ما يجعل الاعتداء عليها ذا طبيعة مركبة تمس المال العام والمرفق العام والأمن القومي في الوقت نفسه.

وقد أكدت الدراسات العربية الحديثة هذا الارتباط؛ إذ أظهرت أن الأمن السيبراني لم يعد مسألة فنية مستقلة عن وظائف الدولة، وإنما أصبح من أدوات حماية النظام العام الرقمي والمرافق والخدمات الأساسية، كما أصبح عنصراً من عناصر الأمن الوطني والقومي بسبب ارتباط الاقتصاد والإدارة والبنية التحتية الحيوية بالأنظمة المعلوماتية (عبد الوهاب، 2026؛ عصمان، 2025).

وتزداد أهمية هذا التصور في البيئة الليبية بعد صدور قرار مجلس الوزراء رقم (358) لسنة 2026 بشأن إنشاء الهيئة الوطنية للأمن السيبراني والسيادة الرقمية، إذ ربط القرار بصورة مباشرة بين حماية البنية التحتية المعلوماتية ومواجهة الهجمات السيبرانية وبين المحافظة على الأمن القومي واستقرار عمل مؤسسات الدولة.

أولاً: مفهوم الأمن القومي وتطور نطاقه:

يعد الأمن القومي من المفاهيم التي شهدت تطوراً كبيراً في الفكر السياسي والقانوني. ففي المفهوم التقليدي كان الأمن القومي يرتبط بصورة أساسية بحماية إقليم الدولة وسيادتها من الاعتداءات العسكرية الخارجية، إلا أن تطور طبيعة التهديدات أدى إلى اتساع نطاقه ليشمل أبعاداً سياسية واقتصادية واجتماعية ومعلوماتية وتقنية.

وقد أصبح أمن الدولة في العصر الحديث مرتبطاً بقدرتها على حماية مؤسساتها الحيوية وضمان استمرار مواردها الاقتصادية وتأمين بياناتها وأنظمتها الرقمية. ومن ثم، فإن التهديد الذي يستهدف النظام المالي أو شبكة الاتصالات أو أنظمة الطاقة أو قواعد البيانات السيادية قد تكون له آثار تماثل في خطورتها بعض صور الاعتداء التقليدي على الدولة.

ويرى جانب من الأدبيات العربية أن التهديدات السيبرانية أدت إلى إعادة تشكيل مفهوم الأمن القومي، لأن الفضاء السيبراني أتاح إمكان التأثير في المؤسسات والاقتصادات والمصالح الحيوية للدول دون الحاجة إلى استخدام القوة العسكرية التقليدية (ربيعي والحروب، 2022، ص 178 وما بعدها؛ مختار، 2015، ص ص 3-32).

ومن ثم، يمكن النظر إلى الأمن القومي في البيئة الرقمية باعتباره قدرة الدولة على حماية سيادتها ومؤسساتها ومواردها وبنيتها التحتية الحيوية وبياناتها وأنظمتها المعلوماتية من التهديدات التي يمكن أن تؤثر في استقرارها أو استقلال قرارها أو استمرار وظائفها الأساسية.

ثانيًا: الأمن السيبراني باعتباره أحد أبعاد الأمن القومي:

أصبح الأمن السيبراني أحد المكونات الرئيسية للأمن القومي؛ لأن الاعتماد على الأنظمة المعلوماتية أصبح شاملاً للعديد من القطاعات ذات الطابع الاستراتيجي، مثل القطاع المالي والمصرفي والطاقة والنفط والاتصالات والنقل والخدمات العامة.

وقد خلصت دراسة عصمان إلى أن الهجمات السيبرانية التي تعرضت لها مؤسسات ليبية، ومن بينها مصرف ليبيا المركزي والمؤسسة الوطنية للنفط، كانت لها آثار سلبية على المؤسسات المستهدفة، وأن خسائرها وانعكاساتها تمتد إلى الأمن القومي والاستقرار، وهو ما يؤكد أن الأمن السيبراني أصبح من أولويات حماية الدولة الليبية (عصمان، 2025). كما يؤكد القانون رقم (5) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية هذا الاتجاه، إذ جعل من أهدافه تحقيق الأمن المعلوماتي وحماية الاقتصاد الوطني وحفظ الحقوق المرتبطة بالاستخدام المشروع للتقنيات وتعزيز الثقة في المعاملات الإلكترونية. وهذه الأهداف تكشف عن أن الحماية التي يستهدفها القانون لا تتعلق بالأفراد وحدهم، وإنما تمتد إلى المصالح الاقتصادية والمؤسسية للدولة.

ويظهر هذا الارتباط بصورة أوضح في قرار مجلس الوزراء رقم (358) لسنة 2026، إذ نصت المادة (3) على أن الهيئة الوطنية للأمن السيبراني والسيادة الرقمية تهدف إلى وضع السياسات والاستراتيجيات والمعايير الوطنية المنظمة للأمن السيبراني وحماية أمن المعلومات والسيادة الرقمية وتأمين البنية التحتية المعلوماتية ومواجهة التهديدات والهجمات، بما يضمن المحافظة على الأمن القومي واستقرار عمل مؤسسات الدولة.

وبعني ذلك أن التنظيم الليبي الحديث اعترف بصورة مباشرة بالطبيعة القومية للأمن السيبراني، ولم يعد ينظر إليه باعتباره مجرد مجال تقني أو جنائي.

ثالثًا: العلاقة بين حماية الأموال العامة والأمن القومي:

تعد الأموال العامة إحدى الدعائم الأساسية لقيام الدولة بوظائفها، ولذلك فإن الإضرار بها على نطاق واسع يمكن أن يؤدي إلى انعكاسات تتجاوز الخسارة المالية المباشرة.

فإذا استهدف هجوم سيبراني نظامًا مرتبطًا بالموازنة العامة أو حسابات الدولة أو الإيرادات العامة أو الرواتب أو القطاع النفطي أو النظام المصرفي، فقد يؤدي ذلك إلى تعطيل عمليات مالية أساسية أو خسارة موارد أو الإضرار بالاستقرار الاقتصادي.

ومن هنا يمكن التمييز بين مستويين للاعتداء السيبراني على المال العام:

- الأول: هو الاعتداء المالي المحدود الذي يقتصر أثره على خسارة مالية في جهة معينة دون أن يؤدي إلى تأثير جوهري في وظائف الدولة أو المرفق العام.
 - أما الثاني: فهو الاعتداء ذي البعد القومي الذي يطل أموالاً أو أنظمة مرتبطة بمؤسسات استراتيجية أو قطاعات حيوية أو يتسبب في تعطيل واسع أو خسائر كبيرة أو آثار ممتدة إلى الاقتصاد الوطني.
- ومن ثم، لا يتحول كل هجوم على المال العام تلقائيًا إلى تهديد للأمن القومي، وإنما يعتمد ذلك على طبيعة الجهة المستهدفة، وحجم الضرر، وامتداد الآثار، وأهمية المال أو النظام محل الهجوم بالنسبة إلى وظائف الدولة.

رابعًا: مفهوم المرفق العام وأهميته:

يمثل المرفق العام أحد المفاهيم الأساسية في القانون الإداري، ويقصد به النشاط الذي تتولاه الدولة أو أحد الأشخاص العامة، أو تشرف عليه، بهدف إشباع حاجة عامة وتحقيق مصلحة جماعية. ويرى الفقه الإداري العربي أن فكرة المرفق العام ترتبط بقيام الدولة بتقديم الخدمات الأساسية للأفراد بصورة منتظمة، وأن المرفق يشكل أحد الأسس التي يقوم عليها القانون الإداري (الطماوي). ولا تقتصر المرافق العامة اليوم على الصور التقليدية، بل أصبحت كثير من خدماتها تعتمد على الوسائل الرقمية والمنصات الإلكترونية وقواعد البيانات والشبكات الحكومية.

ومع توسع التحول الرقمي أصبح وجود المرفق العام واستمراره في حالات كثيرة مرتبطاً بسلامة نظامه الإلكتروني. ولذلك فإن تعطيل النظام التقني قد يؤدي عملياً إلى تعطيل المرفق نفسه حتى لو ظلت مبانيه وموظفوه وأمواله المادية قائمة.

خامسًا: المبادئ القانونية الأساسية التي تحكم المرافق العامة:

يقوم النظام القانوني للمرافق العامة على مجموعة من المبادئ المستقرة في الفقه والقضاء الإداري، من أهمها:

1. مبدأ الاستمرار والانتظام: يقصد بهذا المبدأ أن المرفق العام يجب أن يعمل بانتظام واضطراد، لأن الخدمات التي يؤديها ترتبط بحاجات أساسية للجمهور ولا يجوز أن تتوقف بصورة غير مبررة. ويعد هذا المبدأ من أكثر المبادئ ارتباطاً بموضوع الدراسة؛ إذ يمكن للهجوم السيبراني أن يؤدي إلى توقف النظام الإلكتروني للمرفق وتعذر تقديم الخدمة، حتى دون وقوع اعتداء مادي على منشأته.
2. مبدأ المساواة أمام المرفق العام: يقتضي هذا المبدأ معاملة المتفاعلين بصورة متساوية متى تماثلت مراكزهم القانونية. وفي البيئة الرقمية، قد تؤدي بعض الهجمات إلى تعطيل الخدمة عن فئة أو منطقة معينة أو فقدان بيانات بعض المستفيدين، وهو ما قد ينعكس على القدرة على ضمان المساواة في الحصول على الخدمة.
3. مبدأ قابلية المرفق للتغيير والتطوير: يجب أن تتكيف المرافق العامة مع المتغيرات الاقتصادية والاجتماعية والتكنولوجية، ومن ثم فإن الانتقال إلى الإدارة الرقمية يمثل أحد صور تطور المرفق. غير أن هذا التطور يفرض في المقابل التزامًا بتطوير وسائل الحماية، لأن الرقمنة دون تأمين كافٍ قد تجعل المرفق أكثر عرضة للانقطاع والهجوم.

سادساً: التحول الرقمي للمرفق العام:

أدى التحول الرقمي إلى تغير جوهري في وسائل تقديم الخدمات العامة، فأصبحت المرافق تعتمد على المواقع والمنصات وقواعد البيانات والخدمات الإلكترونية في التواصل مع المستفيدين وإدارة مواردها. وأدى هذا التطور إلى ظهور مفهوم **المرفق العام الإلكتروني**، الذي يقوم على استخدام التقنيات الرقمية في تقديم الخدمة العامة وإدارتها.

وقد تناولت الدراسات العربية المبادئ الضابطة للمرفق العام الإلكتروني، وأكدت استمرار خضوعه للمبادئ التقليدية للمرافق العامة، ولا سيما الاستمرارية والمساواة والتكيف، مع ضرورة إعادة تفسير هذه المبادئ بما يتناسب مع البيئة التقنية (أونيس، 2021). ومن ثم، فإن الانتقال إلى الخدمات الرقمية لا يلغي قواعد المرفق العام، بل يضيف إليها التزامات جديدة تتعلق بحماية الأنظمة وضمان توفر الخدمة الإلكترونية وعدم تعطيلها.

سابعاً: أثر الهجمات السيبرانية في مبدأ استمرارية المرفق العام:

تعد الهجمات التي تستهدف تعطيل الأنظمة أو حجب الخدمة أو تشفير البيانات من أكثر الصور تأثيراً في استمرارية المرافق العامة. فإذا تعرض نظام إلكتروني تابع لمرفق صحي أو مالي أو اتصالاتي أو إداري للتوقف، فإن الأثر قد يظهر في عدم قدرة المواطنين على الحصول على الخدمة أو تعذر تنفيذ العمليات المالية أو فقدان إمكانية الوصول إلى البيانات اللازمة لتسيير العمل.

وفي هذه الحالة لا يكون الضرر تقنياً فقط، بل يتحول إلى إخلال قانوني بوظيفة المرفق العام. وتبرز هنا أهمية الانتقال من الحماية اللاحقة إلى التدابير الوقائية التي تضمن استمرارية الخدمة، مثل النسخ الاحتياطية، وخطط استمرارية الأعمال، وإدارة المخاطر، وخطط التعافي من الكوارث والهجمات.

ثامناً: الأمن السيبراني كضمان لاستمرارية المرفق العام:

أصبحت حماية النظام المعلوماتي للمرفق إحدى الوسائل الضرورية لضمان استمرار الخدمة العامة. وتدعم الدراسات القانونية الحديثة هذا الاتجاه؛ فقد خلص عبد الوهاب إلى أن الأمن السيبراني يمكن النظر إليه باعتباره مرفقاً عاماً حديثاً يرتبط بحماية النظام الرقمي العام، ويتميز بخصائص الاستمرارية والعمومية وخضوعه لإشراف الدولة (عبد الوهاب، 2026). وتفيد هذه الفكرة في موضوع الدراسة من جانبين: الأول أن الأمن السيبراني يشكل أداة لحماية المرافق الأخرى، والثاني أنه قد يشكل بذاته وظيفة عامة يجب على الدولة تنظيمها وضمان استمرارها. ويظهر الاتجاه نفسه في قرار مجلس الوزراء الليبي رقم (358) لسنة 2026 الذي أنشأ هيئة عامة مستقلة نسبياً تتولى وضع السياسات والمعايير الوطنية ومراقبة أمن الأنظمة الحكومية.

تاسعاً: المرافق العامة الحيوية والحماية السيبرانية:

ليست جميع المرافق متساوية من حيث أثر توقفها. فهناك مرافق يمكن أن يؤدي تعطيلها إلى آثار واسعة على المجتمع والدولة، مثل مرافق:

- الطاقة والنفط.
- الاتصالات.
- القطاع المصرفي والمالي.
- المياه.
- الصحة.
- النقل.
- الموانئ والمطارات.
- قواعد البيانات والسجلات السيادية.

وتتطلب هذه المرافق مستوى أعلى من الحماية لأنها تمثل جزءاً من البنية التحتية الحيوية للدولة. ويؤكد قرار مجلس الوزراء رقم (358) لسنة 2026 هذا الاتجاه عندما أسند إلى الهيئة تأمين الشبكات الحكومية السيادية، ووضع الضوابط الفنية اللازمة لتأمين الأنظمة الحكومية، وتنظيم استضافة البيانات الوطنية والحوسبة السحابية الحكومية، وإدارة الأصول الرقمية الوطنية وحماية الهوية الرقمية.

عاشرًا: البنية التحتية الرقمية كمصلحة وطنية محمية:

أصبحت البنية التحتية المعلوماتية جزءاً لا يتجزأ من البنية التحتية الحديثة للدولة. وقد نص القرار رقم (358) لسنة 2026 صراحة على تأمين البنية التحتية المعلوماتية ضمن أهداف الهيئة، وهو ما يمثل تطوراً مهماً في التنظيم الليبي؛ لأنه ينقل الحماية من التركيز على الجريمة الفردية إلى حماية البنية الرقمية ذاتها. كما تتولى الهيئة، وفق المادة (5)، إدارة منظومة الإنذار المبكر ورصد التهديدات وإجراء اختبارات الاختراق والتحليل الأمني والاستجابة للحوادث، فضلاً عن مراجعة أمن الأنظمة الحكومية والتفتيش على الجهات العامة للتحقق من التزامها بالسياسات والمعايير الوطنية. وتدل هذه الاختصاصات على اتجاه نحو بناء نظام وقائي مؤسسي لا يكتفي بمعاينة الفاعل بعد وقوع الهجوم.

الحادي عشر: الالتزام القانوني للجهات العامة بالحماية السيبرانية:

يطرح التحول الرقمي مسألة مهمة تتمثل في مدى وجود التزام قانوني يقع على الجهات العامة لتأمين أنظمتها. وقد قرر القرار رقم (358) لسنة 2026 التزام جميع الجهات العامة بالتعاون الكامل مع الهيئة الوطنية للأمن السيبراني وتمكينها من ممارسة اختصاصاتها، كما منحها صلاحيات التفتيش والتقييم الأمني وقياس الالتزام ومراجعة الأنظمة وإصدار شهادات

الامتثال الأمني. ومن ثم، يتجه التنظيم الليبي إلى الانتقال تدريجيًا من فكرة أن الحماية السيبرانية مسألة اختيارية أو فنية داخلية إلى اعتبارها التزامًا مؤسسيًا يخضع للرقابة والمعايير الوطنية. ويثير ذلك لاحقًا مسألة المسؤولية عند الإخلال الجسيم بتلك الالتزامات، خاصة إذا ترتب على التقصير ضرر بالمال العام أو توقف مرفق حيوي.

الثاني عشر: التوازن بين متطلبات الأمن القومي وحماية المرفق العام:

قد توجي عبارة «بين متطلبات الأمن القومي وحماية المرفق العام» بوجود تعارض بين المفهومين، إلا أن العلاقة بينهما في هذا الموضوع تقوم في الأصل على التكامل لا التعارض.

فحماية المرفق العام الرقمي تسهم في حماية الأمن القومي، لأن استقرار المؤسسات والخدمات الحيوية يمثل أحد عناصر استقرار الدولة. وفي المقابل، فإن تبني سياسات وطنية للأمن السيبراني يوفر للمرافق العامة إطارًا مشتركًا للحماية والمعايير والاستجابة.

ومع ذلك، قد تظهر بعض مسائل التوازن عندما تتطلب حماية الأمن القومي فرض إجراءات رقابية أو قيود على البيانات أو تشديد متطلبات النفاذ إلى الأنظمة، بينما يقتضي تشغيل المرفق سرعة الوصول إلى المعلومات وتيسير الخدمة. ومن هنا يجب أن تخضع التدابير الأمنية لمبادئ الضرورة والتناسب والمشروعية، بحيث تحقق الغرض الأمني دون تعطيل غير مبرر للخدمة العامة.

الثالث عشر: من حماية المرفق إلى استمرارية الأعمال:

أصبح مفهوم استمرارية المرفق في البيئة الرقمية أوسع من مجرد استمرار الموظفين في أداء وظائفهم، إذ يتطلب استمرار:

1. الوصول إلى البيانات.
2. تشغيل الشبكات.
3. الأنظمة المالية.
4. منصات الخدمات.
5. وسائل الاتصال.
6. أنظمة الحفظ والنسخ الاحتياطي.

ومن ثم، فإن استمرارية الأعمال الرقمية تعد ترجمة حديثة لمبدأ استمرار المرفق العام. ويتطلب ذلك وجود خطط مسبقة للتعامل مع الحوادث، وتحديد الأنظمة الحرجة، وتحديد أولويات الاستعادة، وتوفير أنظمة بديلة ونسخ احتياطية آمنة.

الرابع عشر: الاستجابة للحوادث والتعافي باعتبارهما من متطلبات الحماية القانونية:

لا تكتمل الحماية السيبرانية بمنع الهجوم فقط، لأن منع جميع الهجمات بصورة مطلقة أمر غير واقعي. ولهذا تشمل الحماية الحديثة ثلاثة مراحل مترابطة:

(الوقاية، والاستجابة، والتعافي) وقد انعكس ذلك في القرار رقم (358) لسنة 2026؛ إذ نص على رصد التهديدات وإدارة الإنذار المبكر واتخاذ التدابير اللازمة للاستجابة للحوادث السيبرانية، كما أجاز لرئيس الهيئة اقتراح إنشاء مركز وطني للاستجابة للطوارئ السيبرانية (CERT). ويعد ذلك مهمًا لحماية الأموال العامة، لأن سرعة اكتشاف الهجوم واحتوائه قد تحد من مقدار الضرر المالي وتقلل مدة توقف المرفق.

الخامس عشر: العلاقة بين حماية المال العام واستمرارية المرفق:

لا يمكن الفصل بصورة كاملة بين المال العام والمرفق العام؛ فكثير من الأموال العامة تخصص أصلاً لتمكين المرافق من أداء وظائفها. ومن ثم، فإن الاعتداء على المال قد يعطل المرفق، كما أن تعطيل المرفق قد يؤدي إلى خسائر مالية وإهدار موارد عامة. وفي البيئة الرقمية يصبح هذا الترابط أوضح؛ إذ يمكن لهجوم واحد أن يؤدي في الوقت نفسه إلى:

- تعطيل النظام.
- فقدان البيانات.
- وقف الخدمة.
- تكبد خسائر مالية.
- الإضرار بالثقة في المؤسسة.
- التأثير في قطاع حيوي.

وهذا يبرر الحاجة إلى تبني نموذج قانوني يقوم على الحماية المتكاملة بدل النظر إلى كل أثر بصورة منفصلة.

السادس عشر: معايير اعتبار الهجوم السيبراني تهديدًا للأمن القومي:

لا ينبغي التوسع في وصف كل اعتداء إلكتروني بأنه تهديد للأمن القومي، حتى لا يفقد المفهوم دقته القانونية. ويمكن اقتراح مجموعة من المعايير التي تساعد في التمييز، من أهمها:

1. أن يستهدف الهجوم مؤسسة أو بنية تحتية ذات طبيعة استراتيجية.
2. أن يؤدي إلى تعطيل واسع لخدمة عامة أساسية.
3. أن يسبب خسائر اقتصادية جسيمة.
4. أن يؤثر في قدرة الدولة على ممارسة إحدى وظائفها الأساسية.
5. أن يستهدف بيانات سيادية أو أنظمة حكومية حساسة.

6. أن يكون منظماً أو ممتداً أو عابراً للحدود.
 7. أن يترتب عليه اضطراب اقتصادي أو اجتماعي واسع.
- وتسمح هذه المعايير بالتمييز بين الجريمة الإلكترونية ذات النطاق الفردي والهجوم الذي يرتقي إلى مستوى الخطر القومي.
- السابع عشر: الاتجاه الليبي نحو بناء منظومة وطنية متكاملة:**
- تكشف التشريعات والتنظيمات الليبية الحديثة عن تطور تدريجي نحو بناء منظومة متعددة المستويات للأمن السيبراني. فالقانون رقم (5) لسنة 2022 يمثل المستوى الجنائي من خلال تجريم الاعتداءات الإلكترونية وحماية الاقتصاد والمعاملات. أما قرار مجلس الوزراء رقم (358) لسنة 2026 فيمثل المستوى التنظيمي والوقائي والرقابي، من خلال إنشاء هيئة متخصصة تضع السياسات والمعايير الوطنية وتؤمن الشبكات وتراقب الامتثال وتستجيب للحوادث.
- ويمثل الجمع بين المستويين خطوة مهمة نحو الانتقال من نموذج يركز على العقوبة بعد وقوع الجريمة إلى نموذج يقوم على إدارة المخاطر والوقاية والاستجابة والرقابة. ومع ذلك، تبقى فعالية هذا الإطار مرتبطة بمدى إصدار اللوائح والمعايير التفصيلية وتطبيقها عملياً على الجهات العامة وربطها بنظام واضح للمسؤولية والمساءلة.
- يتبين أن حماية الأموال العامة من الهجمات السيبرانية لا يمكن فصلها عن متطلبات الأمن القومي أو عن المبادئ القانونية التي تحكم المرفق العام. فالأموال العامة تمثل أداة أساسية لممارسة الدولة لوظائفها، والمرافق تعتمد بصورة متزايدة على الأنظمة الرقمية، بينما قد يؤدي تعطيل المؤسسات أو البنية التحتية الحيوية إلى أثار تتجاوز المؤسسة المستهدفة وتمس استقرار الدولة واقتصادها.
- وقد أظهر التنظيم الليبي الحديث تطوراً واضحاً في هذا الاتجاه، وخاصة مع صدور القانون رقم (5) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية وقرار مجلس الوزراء رقم (358) لسنة 2026 بشأن إنشاء الهيئة الوطنية للأمن السيبراني والسيادة الرقمية. وقد ربط القرار الأخير بصورة مباشرة بين حماية البنية التحتية المعلوماتية ومواجهة الهجمات السيبرانية وبين الأمن القومي واستقرار عمل مؤسسات الدولة.
- ومن ثم، فإن الحماية الفعالة للأموال العامة في البيئة الرقمية تقتضي إقامة توازن يقوم على تكامل ثلاثة أهداف: حماية المال العام من الإهدار والاستيلاء، وضمان انتظام المرفق العام واستمراره، والمحافظة على الأمن القومي والسيادة الرقمية للدولة.
- استنتاجات الدراسة:**
1. لم تعد حماية الأموال العامة مقتصرة على الأموال في صورتها المادية، بل امتدت في البيئة الرقمية إلى حماية الأنظمة والمنصات وقواعد البيانات المرتبطة بإدارتها.
 2. يقوم مفهوم المال العام في التشريع الليبي أساساً على ملكية الدولة أو الشخص الاعتباري العام وتخصيص المال للمنفعة العامة.
 3. ما زال التنظيم التقليدي للمال العام بحاجة إلى تطوير ليستوعب بصورة أوضح الأصول الرقمية والبيانات والمنصات الحكومية ذات القيمة المالية أو الاستراتيجية.
 4. يوفر القانون رقم (2) لسنة 1979 بشأن الجرائم الاقتصادية حماية مهمة للأموال العامة من الاختلاس والاستيلاء والإضرار والتقصير في الحفظ، لكنه صيغ أساساً لمواجهة صور الاعتداء التقليدية.
 5. وفر القانون رقم (5) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية أساساً قانونياً لمواجهة صور حديثة من الاعتداء، مثل الدخول غير المشروع، وتعطيل الأنظمة، والتلاعب بالبيانات، والاعتداء على الأدلة الرقمية.
 6. توجد إمكانية للتكامل بين قانون الجرائم الاقتصادية وقانون مكافحة الجرائم الإلكترونية عندما يؤدي الهجوم السيبراني إلى اختلاس أو استيلاء أو إضرار بالمال العام.
 7. أظهر القانون رقم (6) لسنة 2022 بشأن المعاملات الإلكترونية أهمية متزايدة لتنظيم البيئة الرقمية التي تمارس من خلالها الجهات العامة معاملاتها وخدماتها.
 8. لا تكفي الحماية الجنائية اللاحقة وحدها لمواجهة الهجمات السيبرانية، بل تتطلب الحماية الفعالة إجراءات وقائية تشمل إدارة المخاطر، والإنذار المبكر، والاستجابة، والتعافي، واستمرارية الأعمال.
 9. أصبحت الهجمات السيبرانية على المؤسسات المالية والنفطية والمصرفية والاتصالاتية والبنية التحتية الحيوية قادرة على التحول من اعتداء تقني محدود إلى تهديد للأمن القومي.
 10. ترتبط حماية الأموال العامة ارتباطاً وثيقاً بمبدأ استمرارية المرفق العام، لأن تعطيل الأنظمة الرقمية قد يؤدي إلى توقف الخدمات العامة حتى دون الاستيلاء المباشر على الأموال.
 11. مثل إنشاء الهيئة الوطنية للأمن السيبراني والسيادة الرقمية بموجب قرار مجلس الوزراء رقم (358) لسنة 2026 خطوة مهمة نحو بناء منظومة مؤسسية للوقاية والرقابة والاستجابة للهجمات السيبرانية.
 12. خلصت الدراسة إلى أن حماية الأموال العامة من الهجمات السيبرانية تتطلب نظاماً قانونياً متكاملاً واستباقياً يجمع بين حماية المال العام، وضمان استمرارية المرفق العام، والمحافظة على الأمن القومي والسيادة الرقمية للدولة.

توصيات الدراسة:

1. تطوير التشريعات الليبية المنظمة لحماية الأموال العامة بما يستوعب طبيعة البيئة الرقمية، وعدم قصر الحماية على الصور التقليدية للأموال والاعتداءات الواقعة عليها.
2. وضع تعريف قانوني واضح للأصول الرقمية العامة يشمل - وفق ضوابط محددة - البيانات وقواعد المعلومات والمنصات والأنظمة والأصول الرقمية ذات القيمة المالية أو الاستراتيجية المرتبطة بالمرافق العامة.
3. العمل على تحقيق التكامل التشريعي بين قانون الجرائم الاقتصادية رقم (2) لسنة 1979، وقانون مكافحة الجرائم الإلكترونية رقم (5) لسنة 2022، وقانون المعاملات الإلكترونية رقم (6) لسنة 2022، بما يقلل من تداخل النصوص ويحدد نطاق تطبيق كل منها.
4. إصدار إطار تشريعي وطني متكامل للأمن السيبراني يحدد بصورة دقيقة التزامات الجهات العامة ومسؤولياتها في حماية الأنظمة والبيانات والأموال العامة، وآليات الرقابة والمساءلة عند الإخلال بهذه الالتزامات.
5. وضع نظام وطني لتحديد وتصنيف البنية التحتية الرقمية الحيوية، مع إخضاع المؤسسات المالية والمصرفية والنفطية والطاقة والاتصالات وغيرها من المرافق الاستراتيجية لمستويات أعلى والزامية من الحماية السيبرانية.
6. دعم الهيئة الوطنية للأمن السيبراني والسيادة الرقمية وتمكينها من ممارسة اختصاصاتها الرقابية والفنية، مع الإسراع في إصدار اللوائح والمعايير والأدلة اللازمة لتنفيذ قرار مجلس الوزراء رقم (358) لسنة 2026.
7. إلزام الجهات العامة بإجراء تقييمات دورية للمخاطر واختبارات أمنية لأنظمتها وشبكاتها، ومعالجة الثغرات المكتشفة قبل استغلالها في الاعتداء على الأموال أو البيانات العامة.
8. إنشاء نظام واضح وملزم للإبلاغ عن الحوادث السيبرانية، يحدد الجهات التي يجب إبلاغها، والمدة الزمنية للإبلاغ، والمعلومات الواجب تقديمها، وإجراءات الاحتواء والاستجابة والتعافي.
9. تطوير قواعد الإثبات الجنائي الرقمي ووضع معايير وطنية موحدة لجمع الأدلة الإلكترونية وحفظها وتحليلها وتوثيق سلسلة حيازتها، مع تاهيل أعضاء الجهات القضائية والأمنية والرقابية في هذا المجال.
10. إلزام الجهات العامة بوضع خطط لاستمرارية الأعمال والتعافي من الهجمات السيبرانية، بما يضمن استمرار المرافق والخدمات الأساسية وتقليل الخسائر المالية والإدارية عند وقوع الهجوم.
11. تضمين العقود الحكومية المتعلقة بالبرمجيات والاستضافة والحوسبة السحابية والخدمات التقنية شروطاً إلزامية للأمن السيبراني، تتناول حماية البيانات، ومكان استضافتها، والإبلاغ عن الاختراقات، والنسخ الاحتياطي، واستمرارية الخدمة، والمسؤولية عن النقص الأمني.
12. تعزيز التنسيق الوطني والتعاون الدولي بين الهيئة الوطنية للأمن السيبراني والجهات القضائية والأمنية والمالية والرقابية، وتطوير آليات تبادل المعلومات والأدلة والخبرات مع الدول والمنظمات المختصة، بما يعزز حماية الأموال العامة والأمن القومي واستمرارية المرافق العامة من الهجمات السيبرانية العابرة للحدود.

قائمة المراجع:

أولاً: الكتب:

1. آل مواش، ضرغام جابر، جريمة التجسس المعلوماتي: دراسة مقارنة، ط1، المركز العربي للنشر والتوزيع، القاهرة، 2017.
2. حجازي، عبد الفتاح بيومي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر.
3. حجازي، عبد الفتاح بيومي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، مصر.
4. رمضان، مدحت عبد الحليم، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، مصر.
5. الطماوي، سليمان محمد، مبادئ القانون الإداري: دراسة مقارنة، دار الفكر العربي، القاهرة، مصر.
6. عبد الله، عبد الغني بسيوني، القانون الإداري: دراسة مقارنة لأسس ومبادئ القانون الإداري وتطبيقها، منشأة المعارف، الإسكندرية، مصر.
7. عبد الوهاب، محمد رفعت، مبادئ وأحكام القانون الإداري، منشورات الحلبي الحقوقية، بيروت، لبنان.
8. العمري، محمد محمود، مدخل إلى الأمن السيبراني، ط1، دار زهران للنشر والتوزيع، الأردن، 2020.
9. يوسف، يوسف حسن، الجريمة الدولية للإنترنت، المركز القومي للإصدارات القانونية، القاهرة، مصر.

ثانياً: البحوث والدراسات العلمية

10. أونيسي، ليندة، «المبادئ الضابطة للمرفق العام الإلكتروني»، مجلة الحقوق والعلوم الإنسانية، جامعة عباس لغرور خنشلة، الجزائر، المجلد 14، العدد 1، 2021، ص 204 وما بعدها.
11. حامد، سليمة مصباح، «التحديات السيبرانية وانعكاساتها على الأمن القومي الليبي: التأسيس وآليات التحصين المعرفي»، كتاب أبحاث المؤتمر العلمي الدولي الرابع لكلية الاقتصاد والتجارة، المجلد 4، 2023، ص 256-280.
12. ربيعي، حسين؛ الحروب، سمر محمود، «الحروب السيبرانية: المخاطر واستراتيجيات تحقيق الأمن السيبراني الدولي والداخلي»، المجلة الجزائرية للأمن الإنساني، المجلد 7، العدد 2، 2022.

13. عبد الوهاب، نمير علي وآخرون، «الأمن السيبراني كمرفق عام: دراسة في الأساس القانوني والتنظيم الإداري»، المجلة الدولية للبحوث والدراسات القانونية، المجلد 5، العدد 2، 2026.
 14. عقيل، عبد الحكيم عبد العزيز بن جريد، «حوكمة الأمن السيبراني وحماية الهوية الوطنية الليبية: دراسة تحليلية على مصلحة الأحوال المدنية الليبية»، المجلة الليبية للدراسات الأكاديمية المعاصرة، المجلد 4، العدد 1، 2026، ص ص 66-82.
 15. عصمان، الوليد عبد المجيد، «أثر التهديدات السيبرانية على الأمن القومي في ليبيا»، مجلة جامعة درنة للعلوم الإنسانية والاجتماعية، جامعة درنة، ليبيا، المجلد 3، العدد 6، سبتمبر 2025، ص ص 414-440.
 16. الغزير، نعيمة عمر، «حماية الأموال العامة في النظام القانوني الليبي»، مجلة آفاق اقتصادية، كلية الاقتصاد والتجارة، جامعة المرقب، المجلد 3، العدد 5، 2017، ص ص 261-295.
 17. الكيلاني، سراج الدين عبد الله، «الأموال العامة الخاضعة للحماية في ليبيا»، مجلة الأصالة، المجلد 6، العدد 11، 2025.
 18. مختار، محمد، «هل يمكن للدولة أن تتجنب مخاطر الهجمات السيبرانية»، مجلة اتجاهات الأحداث، العدد 6، أبوظبي، 2015، ص ص 3-32.
- ثالثاً: التشريعات والقرارات الليبية**
1. دولة ليبيا، القانون المدني الليبي، الصادر في 28 نوفمبر 1953 وتعديلاته، ولا سيما المادتان (87) و(88) المتعلقة بالأموال العامة.
 2. دولة ليبيا، القانون رقم (2) لسنة 1979 بشأن الجرائم الاقتصادية، ولا سيما المواد (1)، (3)، (9)، (10)، (15)، (27)، (28)، (37).
 3. دولة ليبيا، قانون العقوبات الليبي وتعديلاته، الأحكام المتعلقة بجرائم الاعتداء على الأموال والمصالح العامة.
 4. دولة ليبيا، القانون رقم (5) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية، الصادر بتاريخ 27 سبتمبر 2022.
 5. دولة ليبيا، القانون رقم (6) لسنة 2022 بشأن المعاملات الإلكترونية، 2022.
 6. دولة ليبيا، قرار مجلس الوزراء رقم (358) لسنة 2026 بشأن إنشاء الهيئة الوطنية للأمن السيبراني والسيادة الرقمية، الصادر بتاريخ 15 يوليو 2026، ولا سيما المواد (3-6) و(9) رابعاً: الأحكام القضائية:
 1. المحكمة العليا الليبية، الطعن الإداري رقم (62/43 ق)، جلسة 23 يناير 2000، بشأن نزاع الملكية للمنفعة العامة واكتساب أموال الدولة صفة المال العام.
- خامساً: الوثائق والاتفاقيات والتقارير:**
1. جامعة الدول العربية، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، القاهرة، 2010.
 2. مجلس وزراء الداخلية العرب، الاستراتيجية العربية للأمن السيبراني ومكافحة الجرائم المرتبطة بتقنية المعلومات، تونس.
 3. الهيئة الوطنية لأمن وسلامة المعلومات، الوثائق والتقارير المتعلقة بالأمن السيبراني وأمن وسلامة المعلومات في ليبيا، ليبيا.
 4. المركز الليبي للاستشعار عن بعد وعلوم الفضاء والجهات الوطنية المختصة، تقارير ودراسات متعلقة بأمن المعلومات والبنية التحتية الرقمية في ليبيا، ليبيا.
- سادساً: التشريعات العربية المقارنة:**
1. جمهورية مصر العربية، القانون رقم (175) لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية، العدد 32 مكرر (ج)، 14 أغسطس 2018.
 2. جمهورية مصر العربية، القانون رقم (182) لسنة 2018 بشأن تنظيم التعاقدات التي تبرمها الجهات العامة، الجريدة الرسمية، 2018.
 3. جمهورية مصر العربية، القانون رقم (151) لسنة 2020 بإصدار قانون حماية البيانات الشخصية، الجريدة الرسمية، 2020.
 4. المملكة العربية السعودية، نظام مكافحة جرائم المعلوماتية، الصادر بالمرسوم الملكي رقم (م/17)، بتاريخ 1428/3/8هـ.
 5. دولة الإمارات العربية المتحدة، المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية، 2021.