الجرائم الجنائية للموظف العام في المنظومة الإدارية الإلكترونية
دراسة مقارنة

الباحث / سجى غنيم الزيد
دكتوراه فى القانون العام – كلية القانون – جامعة الشارقة .
والسيد الأستاذ الدكتور / سام سليمان دله
أستاذ القانون العام – كلية القانون – جامعة الشارقة .

ملخص البحث

يهدف البحث إلى تحليل الإطار القانوني للجرائم الجنائية في المنظومة الإدارية الإلكترونية للموظف العام في ثلاث دول هي مصر والكويت ودولة الإمارات العربية المتحدة. ويهدف البحث إلى فهم التشريعات والأنظمة المعمول بها في هذه الدول، وتحليل القوانين والتشريعات المتعلقة بالجرائم الجنائية في المنظومة الإدارية الإلكترونية..

وقد توصل البحث إلى عدد من النتائج، أهمها:أن المشرع المصري أحسن في النص على الحكم بعزل الموظف العام في حال ارتكابه جريمة أثناء وبسبب وظيفته، مما يعزز الثقة والنزاهة المفترضة في شغل المناصب العامة. وأنه لم يتطرق المشرع الكويتي في القانون الكويتي رقم (٦٣) لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات الى توضيح المقصود بالمعلومات الحكومية وسرية المعلومات وتحديدها مثل ما نص عليه المشرع المصري والإماراتي، وعدم وجود نص خاص بتجريم إحجام الشخص الاعتباري عن ابلاغ الجهات الرسمية في حال وقوعه ضحية الجريمة الإلكترونية في القانون المصري والإماراتي والكويتي.

وقد أوصى البحث بضرورة تبني المشرع الكويتي للتجريم بواقعية ووضوع لا لبس ولا غموض فيهما بتفادي أنماط وصور مطاطة من أنواع السلوك في مجال الجرائم الإلكترونية في القانون الكويتي رقم (٦٣) لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات حتى لا تتناقض أسس الحماية الموضوعية أو تتعارض مع بعضها البعض، مع مراعاة المنظور المستقبلي ليتواكب مع التطور السريع في أشكال وأنماط وأدوات الجريمة الإلكترونية (المعلوماتية). كما ينبغي على المشرع الكويتي توضيح المقصود بالمعلومات الحكومية وسرية المعلومات وتحديدها بدقة في القانون الكويتي رقم (٦٣) لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات، لضمان وضوح القواعد القانونية والحماية اللازمة لهذه البيانات والمعلومات على غرار القانون المصري والإماراتي.

Abstract

The legal framework for criminal offenses in the electronic administrative system in the light of the Egyptian, Kuwaiti and Emirati legislation

The research aimed to analyze the legal framework for criminal offenses in the electronic administrative system for public servants in three countries: Egypt, Kuwait and the United Arab Emirates. The research aims to understand the legislation and regulations in force in these countries, and to analyze the laws and regulations related to criminal offenses in the electronic administrative system.

The research reached a number of results, the most important of which are: that the Egyptian legislator was better at stipulating the ruling to dismiss the public employee in the event that he committed a crime during and because of his job, which enhances the trust and assumed integrity in occupying public positions. And that the Kuwaiti legislator in Kuwaiti Law No. (63) of 2015 in the matter of combating information technology crimes did not address the clarification of what is meant by government information and the confidentiality of information and its definition, as stipulated by the Egyptian and Emirati legislators, and the absence of a special text criminalizing the reluctance of a legal person to inform the official authorities in the event Being a victim of cybercrime in Egyptian, Emirati and Kuwaiti law.

The research recommended the need for the Kuwaiti legislator to adopt criminalization with realism, clarity, and unambiguity, by avoiding flexible patterns and images of types of behavior in the field of electronic crimes in Kuwaiti Law No. (63) of 2015 regarding combating information technology crimes so that the foundations of objective protection do not contradict or conflict with each other, taking into account the future perspective to keep pace with the rapid development in the forms, patterns and tools of (informational) cybercrime. The Kuwaiti legislator should also clarify what is meant by government information and the confidentiality of information and define it accurately in Kuwaiti Law No. (63) of 2015 regarding combating information technology crimes, to ensure the clarity of the legal rules and the necessary protection for this data and information, similar to Egyptian and Emirati law.

المقدمة

إن التقدم التكنولوجي السريع الذي يشهده هذا العصر، أصبحت المنظومات الإدارية الإلكترونية جزءاً أساسيًا من العمل الحكومي في العديد من الدول، حيث تعتمد هذه المنظومات على استخدام التكنولوجيا الرقمية لتحسين الكفاءة وتسهيل العمليات الإدارية وتوفير خدمات أفضل للمواطنين.

ويعتبر الموظف العام عنصراً حيوياً في نظام الإدارة الإلكترونية، حيث يمكن أن يكون له تأثير إيجابي أو سلبي على نجاح المرفق العام في تطبيق نظام الإدارة الإلكترونية. فبفضل العاملين المجتهدين والملتزمين في المرفق العام، يمكن أن تعمل الإدارة الإلكترونية بشكل فعال وتحقق النجاح والأرباح. ومن ناحية أخرى، يمكن أن يكون الموظف العام سبباً في تحقيق خسائر مالية كبيرة للمرفق العام في حالة عدم وجود تشريعات واضحة تحدد مسؤوليته القانونية وتفرض عقوبات على انتهاكاته الإلكترونية. وقد يتورط الموظف العام في ارتكاب جرائم إلكترونية خلال أداء عمله، مثل جرائم الاحتيال الإلكتروني التي تشمل التلاعب بالمعلومات أو الاستيلاء على الأموال أو البيانات الشخصية للآخرين بطرق غير قانونية. كما يمكنه تزوير المستندات الرسمية أو الوثائق الإلكترونية للحصول على مزايا غير مشروعة أو لإخفاء أنشطة غير قانونية. بالإضافة إلى ذلك، قد يساء استخدام الموظف العام للمعلومات السرية لأغراض تجسس أو للاستفادة الشخصية. وقد يقوم الموظف العام بتغيير أو تدمير البيانات الإلكترونية لتضليل الآخرين أو لإخفاء أنشطة غير قانونية وغير ذلك من الجرائم.

ومن خلال هذا البحث سوف نوضح ونبين أن المُشرع الكويتي قد أصدر في قانون مكافحة الجرائم الإلكترونية الكويتي رقم ٦٣ لسنة ٢٠١٥ والمُشرع المصرى في القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات والمشرع الإماراتي في القانون الاتحادي رقم (٣١) لسنة ٢٠٢١ بإصدار قانون الجرائم والعقوبات لدولة الإمارات العربية المتحدة العديد من صور الجرائم التي يُمكن للموظف العام إرتكابها مثل جريمة الدخول غير المشروع إلى موقع أو نظام معلوماتي، وجريمة الاعتداء على سلامة البيانات والمعلومات

والنظم المعلوماتية، وسوف نقف على تلك التشريعات بشئ من التحليل والتوضيح لتحليل الإطار القانوني للجرائم الجنائية في المنظومة الإدارية الإلكترونية للموظف العام.

وسنتاول الدراسة من خلال البحث فى القانون الكويتى بصفتى أننى كويتية مع المقارنة فى القانون الإتحادى الإماراتى حيث أننى أدرس فى دولة الإمارات العربية المتحدة مقارنة بالنظام المصرى كأحد أهم الأنظمة القانونية فى الوطن العربى.

أولاً: إشكالية البحث

تشهد المجتمعات البشرية قفزة علمية وتقنية هائلة نتيجة للثورة المعلوماتية التي أحدثتها التكنولوجيا الحديثة. تمتاز هذه الثورة بانفتاحها الكبير على الوجود الإنساني ومداها الواسع، مما أدى إلى تغير جذري في طبيعة حياتنا اليومية.

وفي عصرنا الحالي، نحن نعيش في تجليات تلك الثورة التقنية العالية. فقد دخلنا مرحلة جديدة من التطور التكنولوجي، حيث يتدفق علينا سيل من المعلومات الضخمة والمتنوعة التي تتجاوز قدراتنا الحسية والإدراكية. تلك المعلومات تؤثر بشكل كبير في حياتنا وتساهم في تحول جوانب الوجود الإنساني نفسه.

ومن بين التحولات الكبيرة التي شهدها العصر الحديث، ظهور الإدارة الإلكترونية كنمط حديث للتنظيم والإدارة. وفي هذا السياق، يلعب الموظف العام دوراً حاسماً في تطبيق نظام الإدارة الإلكترونية. إذ يمتلك القدرة على تحقيق النجاح والتقدم في هذا النظام، وفي الوقت نفسه، يمكن أن يكون سبباً في تكبد المرفق العام خسائر مالية كبيرة إذا لم يلتزم بالأنظمة والتعليمات الإلكترونية.

وعليه تتمحور أشكالية الدراسة حول التحليل والمقارنة للإطار القانوني للجرائم الجنائية في المنظومة الإدارية الإلكترونية للموظف العام في ثلاث دول: مصر والكويت ودولة الإمارات العربية المتحدة.

ثانياً: تساؤلات البحث

يثير البحث عدد من التساؤلات الهامة، أهمها ما يلي:

١. ما هي أنواع الجرائم الجنائية الإلكترونية التي يمكن أن يرتكبها الموظف العام في المنظومة الإدارية الإلكترونية؟.

٢. ما هي السلوكيات التي يمكن أن تصنف كجرائم جنائية إلكترونية عندما يتعامل الموظف العام مع المعلومات الحساسة أو البيانات الشخصية للمواطنين؟.

٣. ما هي العقوبات المنصوص عليها في التشريعات المعمول بها في مصر والكويت والإمارات للجرائم الجنائية الإلكترونية المرتكبة من قبل الموظف العام؟.

ثالثاً: أهمية البحث

يحمل هذا البحث أهمية كبيرة نظراً للتطورات السريعة في مجال التكنولوجيا والتحول الرقمي الذي يشهده العالم. وفيما يلي بعض الأهمية المحتملة للدراسة:

- **مساهمة في تحسين الأمان الإلكتروني:** يعتبر فهم الإطار القانوني للجرائم الجنائية في المنظومة الإدارية الإلكترونية أمراً بالغ الأهمية لتعزيز الأمان الإلكتروني. من خلال تحليل التشريعات المصرية والكويتية والإماراتية وتحديد الفجوات والثغرات في هذه القوانين، يمكن تطوير تدابير أمنية فعالة وسياسات ملائمة لحماية المعلومات الحكومية والبيانات الشخصية للمواطنين.
- **تعزيز العدالة ومكافحة الجريمة:** يساهم فهم القوانين والأنظمة المعمول بها في مكافحة الجرائم الجنائية الإلكترونية في المنظومة الإدارية الإلكترونية في تحقيق العدالة. ومن خلال وضع قوانين صارمة وفعالة وتحديد عقوبات مناسبة، ويمكن ردع المرتكبين وتنفيذ العدالة بطريقة تتناسب مع خطورة الجرائم الإلكترونية.
- **تحسين كفاءة العمل الحكومي:** يساهم التحليل والتقييم القانوني لكفاءة الموظف العام والإنتاج الخدمي في المنظومة الإدارية الإلكترونية في تحسين الأداء الحكومي. ومن خلال فهم التشريعات والآليات المتبعة لتقييم الأداء وتحسين الإنتاجية، يمكن تحديد المجالات التي تحتاج إلى تحسين وتنفيذ سياسات وبرامج لتحسين كفاءة الموظفين وتطوير الخدمات الحكومية.
- **توجيه التطور التكنولوجي:** يمكن للدراسة أن تساهم في توجيه التطور التكنولوجي في المنظومة الإدارية الإلكترونية لتحقيق أقصى استفادة من التكنولوجيا مع الحفاظ على الأمان والحماية القانونية من خلال فهم التشريعات والأنظمة القانونية المطبقة، يمكن

توجيه سياسات واستراتيجيات التطوير التكنولوجي لتلبية متطلبات الأمان والحفاظ على السلامة القانونية.

رابعاً: أهداف البحث

تهدف هذه الدراسة إلى تحليل الإطار القانوني للجرائم الجنائية في المنظومة الإدارية الإلكترونية للموظف العام في ثلاث دول هي مصر والكويت ودولة الإمارات العربية المتحدة. ويهدف البحث إلى فهم التشريعات والأنظمة المعمول بها في هذه الدول، وتحليل القوانين والتشريعات المتعلقة بالجرائم الجنائية في المنظومة الإدارية الإلكترونية.

ويشمل البحث تحليل القوانين المصرية والكويتية والإماراتية ذات الصلة بالجرائم الجنائية في المنظومة الإدارية الإلكترونية المرتكبة من قبل الموظف العام، مثل جرائم الاختراق الإلكتروني وسرقة المعلومات وتزوير الوثائق الإلكترونية والاعتداء على البيانات الشخصية والاحتيال الإلكتروني. وسيتم تحليل النصوص القانونية والقوانين ذات الصلة، وتحديد الأحكام والعقوبات المنصوص عليها في هذه القوانين.

خامساً: منهج البحث

لقد اعتمدنا في هذا البحث على مزيجًا من المنهج الوصفي والتحليلي والمقارن. حيث يتم استخدام المنهج الوصفي لوصف وتحليل الإطار القانوني للجرائم الجنائية في المنظومة الإدارية الإلكترونية في كل من مصر والكويت والإمارات. ويتم تحليل القوانين والتشريعات المتعلقة بالجرائم الجنائية الإلكترونية المرتكبة من قبل الموظف العام في تشريعات تلك الدول الثلاث.

سادساً: خطة تقسيم البحث

تم تقسيم البحث وفقاً للتقسيم التالي:

المبحث الأول: ماهية الجريمة الالكترونية.

المبحث الثاني: جرائم الأموال العامة الالكترونية للموظف العام

.

المبحث الأول

ماهية الجريمة الالكترونية

تمهيد وتقسيم:

لقد شهدت الثورة العلمية في مجال الحاسوب والإنترنت ظهور ظاهرة الإجرام المعلوماتي، أو الإجرام الإلكتروني، حيث يتم استغلال وسائط الاتصال الإلكترونية لارتكاب جرائم مختلفة. ويمكن للموظف العام، باستخدام هذه الوسائط، القيام بأعمال احتيالية مثل سرقة الأموال من البنوك أو تزوير المستندات، وكذلك الاعتداء على البيانات الشخصية والتجسس، والغش المعلوماتي الذي يتم عن طريق تلاعب المدخلات أو تعديل البرامج، وأيضاً من خلال النسخ غير المشروعة للبرامج. بالإضافة إلى ذلك، تتعلق الجرائم المتعلقة بعمليات الاحتيال واختراق أمان البيانات وسرقة المعلومات[1].

ولقد خصصنا هذا المبحث لتسليط الضوء على ماهية الجريمة الالكترونية، كمدخلاً لبيان موضوع دراستنا، وذلك بتقسيم هذا المبحث إلى المطلبين التاليين:

- المطلب الأول: مفهوم الجريمة الالكترونية.
- المطلب الثاني: طبيعة الجريمة الالكترونية.

---

[1] – محمد عبد الله إبراهيم، المواجهة الأمنية لجرائم شبكة المعلومات الدولية، أكاديمية الشرطة المصرية، وزارة الداخلية، ٢٠١٦، ص١٤. عبد الفتاح بيومي حجازي، جريمة غسل الأموال بين الوسائط الإلكترونية ونصوص التشريع، دار الفكر الجامعي، الإسكندرية، ٢٠٠٥، ص٥٢.

المطلب الأول

مفهوم الجريمة الالكترونية

هناك تباين في التعريفات المقدمة للجرائم الإلكترونية من قبل الفقهاء والخبراء في المجال. وهذا يرجع إلى تعقيد طبيعة هذه الجرائم وتطور التكنولوجيا المستخدمة في ارتكابها. لذلك، يمكن تقديم عدة اتجاهات في تعريف الجرائم الإلكترونية:

الاتجاه الأول المرتبط بوسيلة ارتكاب الجريمة: يستند هذا الإتجاه إلى وسيلة ارتكاب الجريمة، حيث يتم تحديد الجريمة الإلكترونية عن طريق استخدام الحاسوب كأداة رئيسية في ارتكابها. ومع ذلك، يعتبر هذا الاتجاه محدوداً في نطاقه، حيث يركز على الوسيلة المستخدمة دون النظر إلى الفعل الإجرامي الذي يتم ارتكابه. [٢]

ويتم انتقاد الاعتماد فقط على وسيلة الحاسوب لتعريف الجرائم الإلكترونية، حيث يشير البعض إلى أن الجرائم الإلكترونية تتعلق بالأفعال غير القانونية أو الضارة التي يتم ارتكابها باستخدام الحاسوب كأداة، وليس فقط الاعتماد على الحاسوب نفسه كوسيلة. وبالتالي، لا يمكن تصنيف أي جريمة تستخدم الحاسوب كأداة في ارتكابها على أنها جريمة إلكترونية ببساطة. حيث عرفت بأنها "كل أشكال السلوك غير المشروع أو الضار بالمجتمع

---

[٢] – أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، القاهرة، ٢٠٠٦، ص٨٣؛ جاسم محمد جندل، الجرائم الالكترونية، المعتز للنشر والتوزيع، عمان، ٢٠٢٢، ص١٨.

والذي يرتكب باستخدام الحاسب الآلي" [٣] . وعرفت أيضاً بأنها: "الفعل الإجرامي الذي يستخدم في إقترافه الحاسب الآلي كأداة رئيسية"[٤].

الاتجاه الثاني المرتبط بموضوع الجرائم: يتم تعريف الجرائم الإلكترونية بناءً على نوع الموضوع الذي تستهدفه، مثل جرائم القرصنة الإلكترونية، وجرائم الاعتداء على خصوصية المعلومات، وجرائم الابتزاز الإلكتروني، وغيرها. حيث عرفت الجريمة الإلكترونية بناءً على موضوعها على أنها "النشاط الموجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب الآلي أو المعلومات التي تنقل عبره". [٥] ويمكن أيضًا تعريف الجرائم الإلكترونية بأنها "مجموعة الجرائم المتصلة بمعرفة ومعالجة المعلومات اللوجيستية".[٦]

وهذا الاتجاه يعتمد على المعلومات المحل للجريمة الإلكترونية كمعيار لتعريفها، وتعرض هذه النقطة للانتقاد بحيث يشير النقاد إلى أن الحاسوب يلعب دوراً هاماً في وقوع هذه الجرائم، وليس فقط المعلومات المحتواة فيه. وتعريف الجرائم الإلكترونية بالاعتماد على موضوعها يبرز أهمية المعلومات المستهدفة والمعالجة اللوجيستية لها. ومع ذلك، يجب أن يؤخذ في الاعتبار أن الحاسوب نفسه يعد جزءًا أساسيًا في وقوع هذه الجرائم وأنه لا يتم تجاهل هذا الجانب في التعريف. لذا، يفضل أن يتم تعريف الجرائم الإلكترونية بشكل يشمل وجهات النظر المتعددة للحاسوب والمعلومات المتصلة به. [٧]

الاتجاه الثالث المرتبط بالمعرفة الفنية: يتم تعريف الجرائم الإلكترونية بناءً على المعرفة الفنية واستخدام الحوسبة في ارتكابها، مثل جرائم الاختراق الإلكتروني بواسطة الاستغلال الضعيف في الأمان، وجرائم استخدام البرمجيات الخبيثة، وغيرها. ويركز هذا الاتجاه على

---

[٣] – عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دار الكتب القانونية، القاهرة، ٢٠٠٧، ص ٢٤؛ نسرين محمد نعمة الحسيني، الجرائم الالكترونية الواقعة على المال، المكتب الجامعي الحديث، القاهرة، ٢٠٢٠، ص٢٨.

[٤] –سيد علي السيد محمد، الجرائم الالكترونية، دار التعليم الجامعي، القاهرة، ٢٠٢٠، ص ٣.

[٥] – محمد عبد الله أبو بكر، موسوعة جرائم المعلوماتية، جرائم الكمبيوتر والإنترنت، منشأة المعارف، الإسكندرية، ٢٠٠٦ ، ص ١٠.

[٦] – سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الإسكندرية، ٢٠١٥، ص ٢٧.

[٧] – جاسم محمد جندل، مرجع سابق، ص٣٠.

مستوى المعرفة التقنية التي يتحتم على الجاني أن يكون بها لارتكاب الجريمة الإلكترونية. بمعنى آخر، يعتبر فاعل الجريمة مطلوباً أن يمتلك معرفة خاصة بتقنية أنظمة المعلومات لتنفيذ الجريمة. [٨]

وتم تعريف الجرائم الإلكترونية وفقًا لهذا الاتجاه بأنها "جريمة تتطلب لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية النظام المعلوماتي"[٩] و "أي فعل مشروع تكون المعرفة بتقنية الكومبيوتر أساسية لارتكابه والتحقيق فيه وملاحقته قضائيًا".[١٠] وتم استخدام هذا التعريف أيضًا من قبل وزارة العدل الأمريكية التي عرفت الجريمة الإلكترونية بأنها "أي جريمة تتطلب من الفاعل أن يكون لديه معرفة تقنية بالحاسوب لارتكابها".[١١]

ومع ذلك، يتم انتقاد هذا الاتجاه لأنه يقتصر على قدرة الفاعل التقنية فقط، وهو لا يأخذ في الاعتبار أن هناك حالات يمكن للجاني أن يرتكب الجريمة الإلكترونية دون الحاجة إلى مستوى عالٍ من المعرفة الفنية. فعلى سبيل المثال، يمكن لشخص غير متخصص أن يستخدم أدوات بسيطة لاختراق حسابات البريد الإلكتروني أو للقيام بالتصيد الاحتيالي عبر الإنترنت بدون الحاجة إلى مهارات تقنية متقدمة. [١٢]

الاتجاه الرابع المرتبط بمزيج من المعايير: يمكن أن يتم تعريف الجرائم الإلكترونية بناءً على مزيج من المعايير المذكورة أعلاه، حيث يؤخذ في الاعتبار وسيلة ارتكاب الجريمة وموضوعها والمعرفة الفنية المشتركة فيها. [١٣]

هذا الاتجاه في تعريف الجرائم الإلكترونية يستند إلى مزيج من أداة ارتكاب الجريمة وموضوعها. يعرف أنصار هذا الاتجاه الجرائم الإلكترونية بأنها "أي عمل غير مشروع يتسبب في الضرر للأشخاص والأموال ويستهدف التكنولوجيا المتقدمة لأنظمة المعلومات" [١٤]. ويتم

---

[٨] – سيد علي السيد محمد، مرجع سابق، ص٣٢.

[٩] – محمد عبيد الكعبي، الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٧، ص ٣٢.

[١٠] – محمد عبد الله أبو بكر سلامة، مرجع سابق، ص ١٢.

[١١] – أحمد خليفة الملط، مرجع سابق، ص ٩٦.

[١٢] – محمد عبد الله أبو بكر سلامة، مرجع سابق، ص ١١.

[١٣] – محمود أحمد محمد القرعان، الجرائم الالكترونية، دار وائل للبطاعة والنشر، عمان، ٢٠١٧، ص٣٥.

[١٤]– محمد عبد الله أبو بكر سلامة، مرجع سابق، ص ١٤.

التركيز في هذا التعريف على العمل غير المشروع الذي ينشأ عن استخدام غير مشروع لتقنية المعلومات ويهدف إلى الاعتداء على الممتلكات المادية والمعنوية. ويشمل ذلك الأضرار التي تلحق بمكونات الحاسوب وشبكات الاتصال الخاصة به. كما عرفت بأنها "عمل أو إمتناع يأتيه الإنسان أضراراً بمكونات الحاسب المادية والمعنوية وشبكات الإتصال الخاصة به باعتبارها من المصالح والقيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها". (١٥)

وهذا الاتجاه قد حظي بقبول من الفقهاء لأنه يعتمد على معايير متعددة في تعريف الجريمة الإلكترونية ويأخذ في الاعتبار كلًا من الحاسوب كأداة لارتكاب الجريمة والمعلومات التي تتعلق بها الجريمة. يحظى هذا الاتجاه بتأييد جزء من الفقهاء المصريين أيضًا لأنه يعرف الجريمة الإلكترونية بطريقة تعكس واقعها التقني الفريد.

ونحن نرى، أنه من الواضح أن هناك تنوعًا في التعاريف والاتجاهات المستخدمة في تعريف الجرائم الإلكترونية. وعلى الرغم من عدم وجود تعريف جامع وموحد حتى الآن، إلا أن هذه الاتجاهات المختلفة تساهم في فهم طبيعة ونطاق الجرائم الإلكترونية ومساعدة القانونيين والفقهاء في التعامل معها.

وقد أخذ مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين الذي عقد في فيينا عام ٢٠٠٠ بهذا الإتجاه إذ عرف الجرائم الإلكترونية بأنها: "أي جريمة يمكن ارتكابها باستخدام نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي أو شبكة حاسوبية، وتشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية" (١٦)كما عرفت وفقتاً لهذا الإتجاه بأنها:" هي كل نشاط إجرامي يؤدي فيه نظام الحاسب الآلي دورا فيه، سواء تمثل هذا الدور في إتمام النشاط الإجرامي أو في كونه محلا له "(١٧) .

ونحن نرى، بعد استعراض هذه الاتجاهات المختلفة لتعريف الجرائم الإلكترونية، يمكننا الاستنتاج أنه من الصعوبة الاعتماد على معيار واحد فقط لتعريف هذه الجرائم. وإذا اعتمدنا على الاتجاه الأول الذي يستند إلى وسيلة ارتكاب الجريمة، وسنضم جرائماً تقليدية تستخدم الحاسوب كأداة رئيسية في ارتكابها مثل جرائم التزوير التقليدية. أما الاتجاه الثاني

---

(١٥)– عبير شفيق الرحباني، الجرائم الالكترونية ومخاطرها، دار الثقافة للنشر والتوزيع، عمان، ٢٠٢٠، ص٣١.

(١٦) – نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، عمان، ٢٠٠٨، ص ٥٠.

(١٧) – محمد عبد الله أبو بكر سلامة، مرجع سابق، ص١٥.

الذي يعتمد على محل الجريمة كأساس للتعريف، فهو غير كاف وغير دقيق لأنه يتجاهل دور الحاسوب وشبكة الإنترنت في الجرائم الإلكترونية.

وبالنسبة للاتجاه الثالث الذي يعتمد على المعرفة الفنية في استخدام الحاسوب، فإنه لا يعد طريقة مثلى أيضاً، حيث يفترض أن يكون للجاني معرفة واسعة بالحاسوب. وبالتالي، يتطلب البحث في الظروف الشخصية للجاني، وهذا لا يتماشى مع مبدأ القانون الجنائي الذي يعتمد على العمل الموضوعي. بالإضافة إلى ذلك، يحصر هذا الاتجاه المرتكبين في فئة معينة، في حين أن هناك جرائم لا تتطلب معرفة تقنية متقدمة بأمور الحاسوب، مثل جريمة الإتلاف المعلوماتي.

أما الاتجاه الرابع، الذي يعتمد على معياري الأداة والموضوع كأساس لتعريف الجرائم الإلكترونية، فإنه الاتجاه الأكثر دقة وموضوعية. يعتبر الحاسوب أداة مهمة لارتكاب الجرائم الإلكترونية التي تتعلق بالبيانات الإلكترونية. هذا الاتجاه يقدم نظرة شاملة ومتكاملة للجرائم الإلكترونية، حيث يعتبر الحاسوب أداة أساسية لارتكاب هذه الجرائم ويأخذ في الاعتبار أيضاً موضوع الجريمة.

وباستخدام هذا الاتجاه، يتم تعريف الجرائم الإلكترونية بأنها أي فعل غير قانوني ينشأ عن استخدام غير مشروع لتقنية المعلومات، وهذا الفعل يؤدي إلى الإعتداء على المكونات المادية والمعنوية للحاسوب وشبكات الاتصال المرتبطة به. يركز هذا التعريف على الأداة (الحاسوب) والموضوع (البيانات الإلكترونية) ويأخذ بعين الاعتبار تقدم التكنولوجيا وتطورها المستمر.

لذلك، يمكن القول إن الاتجاه الرابع هو الأكثر شمولية وتطابقاً مع واقع الجرائم الإلكترونية. يعكس هذا الاتجاه تفاعل المجتمع الدولي والقانوني مع التحديات الناشئة من التكنولوجيا الرقمية ويساعد في تحديد نطاق الجرائم الالكترونية.

المطلب الثاني

طبيعة الجريمة الالكترونية

تتميز الجريمة الالكترونية بطبيعتها التي تتعلق بالبيئة الرقمية ومعالجة البيانات. فعند وقوع هذه الجرائم، فإن المعلومات تكون الموضوع الأساسي للاعتداء، حيث تتمثل المعلومات في نبضات إلكترونية ويتعين التعامل معها عن طريق معالجة البيانات الإلكترونية[١٨]. ويمكن

[١٨] – نسرين محمد نعمة الحسيني، مرجع سابق، ص٣٦.

للمستخدم أن يقوم بإدخال هذه البيانات إلى الحاسوب ومعالجتها بطرق مختلفة مثل التعديل والتصحيح والمحو والتخزين والاسترجاع والطباعة. وتترتب على هذه العمليات تبعات مرتبطة بارتكاب الجرائم الالكترونية، وبالتالي يجب على الجاني أن يفهم هذه العمليات بشكل جيد، مثل في حالات التزوير والتقليد.[١٩]

تتميز الجرائم الالكترونية عن الجرائم التقليدية بطابعها الخاص وصعوبة كشفها وإثباتها، ويعود ذلك إلى عدة أسباب:

١. **خفية الجرائم الالكترونية:** تتمتع الجرائم التي تحدث على الأنظمة الحاسوبية أو من خلالها، مثل جرائم الإنترنت، بطابع مستتر وخفي، حيث يكون المجني عليه غالباً غير مدرك لوقوع الجريمة أو يجهلها تماماً. ويعود ذلك إلى تعقيد وتطور الطرق المستخدمة في اختراق أنظمة الحاسوب والاعتداء عبر الإنترنت، فضلاً عن استخدام الفيروسات الإلكترونية ووسائل أخرى للتسلل والاختراق[٢٠].

٢. **التطور السريع لأساليب ارتكاب الجرائم الرقمية:** تتسم الجرائم الرقمية بالتطور السريع لأساليبها وتقنياتها. يعود ذلك إلى التقدم التكنولوجي المستمر وتطور الأجهزة والبرمجيات والاتصالات. ويتعلم المجرمون المتخصصون في الجرائم الالكترونية طرقاً جديدة لاختراق الأنظمة والاستيلاء على المعلومات وتنفيذ عمليات احتيال. كما يتم تبادل الخبرات والأدوات اللازمة للقيام بالجرائم عبر المنتديات السوداء والمجتمعات السرية على الإنترنت. هذا التطور السريع يشكل تحدياً للجهات المعنية بمكافحة الجرائم الرقمية لمواكبة ومواجهة تلك الأساليب المتطورة. [٢١]

٣. **التنوع والتعددية في أنواع الجرائم الرقمية:** تشمل الجرائم الالكترونية مجموعة متنوعة من الأنشطة الإجرامية مثل اختراق الأنظمة، وسرقة البيانات، والاحتيال الإلكتروني، وانتشار الفيروسات والبرمجيات الخبيثة، والتهديدات السيبرانية، والتحريض على الكراهية عبر الإنترنت، والتجسس الإلكتروني، والابتزاز الإلكتروني، والاعتداء على الخصوصية الإلكترونية. تعد هذه التنوع والتعددية في أنواع الجرائم

---

[١٩] – عفيفي كامل، مرجع سابق، ص١٨.

[٢٠] – وسيم حسام الدين الأحمد، شرح قانون مكافحة الشائعات والجرائم الالكترونية لدولة الإمارات العربية المتحدة، مرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١، دار الحافظ للنشر والتوزيع، الإمارات، ٢٠٢٣، ص ٣٦.

[٢١] – محمد عبد الله أبو بكر سلامة، مرجع سابق، ص١٥.

الرقمية تحدياً إضافياً في مجال مكافحة الجرائم الرقمية، حيث يتعين على الجهات المختصة تطوير استراتيجيات وأدوات متعددة للكشف عنها ومعاقبة الجناة.

٤. **الجريمة الرقمية عابرة للحدود:** يتميز الجاني في الجرائم الالكترونية بالقدرة على ارتكاب الجريمة والتعامل مع الضحايا والمعلومات عبر الإنترنت، مما يجعلها تتجاوز الحدود الجغرافية بين الدول. فالشبكة العالمية (الإنترنت) تمكن الجناة من الوصول إلى الضحايا في أي مكان في العالم، وتنفيذ الاحتيالات وسرقة المعلومات عبر الحدود بسهولة. وبالتالي، تعد الجرائم الرقمية تحدياً للسلطات القانونية، حيث يصعب تحديد مكان الجاني وتتبعه وتقديمه للعدالة، وقد يتطلب التعاون الدولي وتبادل المعلومات لمكافحة هذه الجرائم بفعالية. [٢٢]

٥. **التحديات التقنية:** يواجه المحققون والمحترفون في مجال مكافحة الجرائم الالكترونية تحديات تقنية كبيرة في استرجاع الأدلة الرقمية وجمع الأدلة القوية اللازمة لإثبات الجريمة. فمع تزايد تعقيد التقنيات المستخدمة في الجرائم الالكترونية، يصبح من الصعب تتبع وتحديد هوية الجناة وتوثيق أدلة قاطعة، وتتمثل التحديات في الآتي:

- **افتقاد الآثار التقليدية للجريمة:** في معظم الجرائم الرقمية، لا توجد آثار خارجية أو مادية تشير إلى وقوع الجريمة أو هوية الجاني. على سبيل المثال، لا توجد جثث أو دماء تدل على جريمة رقمية. وهذا يجعل من الصعب توجيه الاتهام وإثبات الجريمة.
- **غياب الدليل المرئي والمقروء:** معظم البيانات والمعلومات التي تتعامل في الجرائم الرقمية تكون في شكل رموز وتخزن على وسائط تخزين رقمية. يصعب فهمها أو قراءتها بواسطة الإنسان ويتطلب توظيف الحواسيب والبرمجيات لتفسيرها وتحليلها. هذا يزيد من تعقيد جمع الأدلة والتوصل إلى أدلة قوية لدعم القضية.
- **الوصول المحدود إلى الدليل:** المجرمون الرقميون يستخدمون تدابير أمنية لحماية أنفسهم، مثل استخدام كلمات مرور وتشفير البيانات. يصعب الوصول إلى هذه الأدلة المحمية بوسائل تقنية متقدمة، ويتطلب توظيف خبراء الأمن الرقمي المتخصصين للتعامل مع تلك التحديات[٢٣].

---

[٢٢] – ذياب البداينة، الجرائم المستحدثة والبحث العلمي في المجتمع العربي، بحث مقدم للندوة العلمية حول دور البحث العلمي في معالجة مشكلة الجريمة والإنحراف في الدول العربية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ٢٠١٠ ، ص ٣٤.

[٢٣]– عفيفي كامل، جرائم الكمبيوتر، مرجع سابق، ص٣٨-٣٩.

- **سهولة محو الدليل أو تدميره:** يمكن للجاني في الجرائم الرقمية محو الأدلة أو تدميرها بسرعة كبيرة باستخدام تقنيات متقدمة.

٦. **التحديات القانونية:** يواجه النظام القانوني تحديات في مواجهة الجرائم الالكترونية بسبب طبيعتها الحدودية والدولية، حيث يمكن أن تحدث هذه الجرائم عبر الحدود ومن دولة إلى أخرى، مما يصعب عملية التعاون القضائي وتبادل المعلومات والأدلة بين الدول المختلفة.

٧. **طبيعة الأساليب المستخدمة لارتكاب الجريمة الالكترونية:** تتميز الجريمة الالكترونية بالأساليب الفنية والتقنية المستخدمة في ارتكابها، والتي تختلف باختلاف الأهداف والأنظمة المستهدفة. ويقوم مرتكبو الجرائم الالكترونية بتطوير واستخدام وسائل متطورة وغير معتادة للاختراق والاستيلاء على المعلومات أو تعطيل الأنظمة. **وتشمل الأساليب المستخدمة في الجرائم الرقمية ما يلي:**

أ- **الأساليب المستخدمة للاعتداء على المكونات المادية للحاسب:** تشمل هذه الأساليب استهداف المكونات المادية للحاسب وإلحاق الضرر بها. تتضمن بعض الأمثلة على هذه الأساليب:

- **سرقة الدعامة المادية:** يتعمد المجرمون سرقة الدعامة المادية للحاسب، والتي تحتوي على البرامج والبيانات. يمكن استغلال هذه البيانات لأغراض غير قانونية مثل الاحتيال أو السرقة الهوية.
- **سرقة البطاقة الممغنطة:** يستخدم المجرمون وسيلة السحب النقدي أو الحصول على سلع وخدمات من خلال سرقة البطاقة الممغنطة المستخدمة في الحوالات المالية أو الدفعات.
- **إتلاف البرامج والبيانات:** يمكن للمجرمين تدمير البرامج والبيانات المخزنة على الحواسيب بطرق تقليدية مثل إتلاف الدعامات المادية باستخدام الحرق أو الضرب بأدوات ثقيلة، أو تلف الأجزاء الحساسة بسبب سكب سوائل ساخنة عليها.
- **تخريب الأجهزة القارئة:** يمكن للمجرمين لصق ورق صنفرة على أجزاء البطاقات المثقبة المستخدمة في القراءة، مما يتسبب في تلف الأجهزة القارئة وعرقلة وظيفتها.
- **إتلاف الشرائط الممغنطة:** يمكن للمجرمين التسبب في تلف الشرائط والأقراص الممغنطة المستخدمة لتخزين البيانات بواسطة رمي الرماد المشتعل أو الضغط عليها بأدوات حادة.

ب-الأساليب المستخدمة للاعتداء على المكونات الغير مادية للحاسب: تشمل هذه الأساليب استهداف المكونات غير المادية للحاسب واستغلالها بطرق مختلفة. يمكن تصنيفها على النحو التالي [٢٤]:

- **الاطلاع البصري والتنصت:** قد يقتصر الاعتداء على المكونات غير المادية للحاسب على مجرد الاطلاع البصري على المعلومات المعروضة على الشاشة أو التنصت عليها عن طريق استخدام وسائط مثل الكاميرات أو الأجهزة المساعدة لتكبير الصوت الصادر من الحاسب، مما يتيح للمهاجم الوصول المباشر إلى المعلومات المراد سرقتها.
- **السطو الإلكتروني:** يتطلب هذا النوع من الاعتداء معرفة فنية خاصة، حيث يقوم المهاجم بالتقاط أو تسجيل المعلومات والبيانات أثناء انتقالها وبثها من الحاسب إلى طرفية أخرى عبر شبكة الاتصالات. ويمكن استخدام أجهزة احتيالية أو تقنيات الاختراق للوصول إلى هذه المعلومات واستغلالها لأغراض غير قانونية.
- **الهجمات الإلكترونية المتقدمة:** تشمل هذه الأساليب استخدام تقنيات متقدمة لاختراق الأنظمة الحاسوبية واستغلال الثغرات الأمنية. وقد يتم استهداف البرمجيات والتطبيقات الضعيفة أو تنفيذ هجمات الاستنساخ أو الاحتيال الإلكتروني للوصول إلى المعلومات الحساسة.

ونحن نرى، أن أنواع الجرائم الإلكترونية متنوعة وتشمل الاختراق الإلكتروني، والاحتيال الإلكتروني، والتجسس، وانتشار البرمجيات الضارة، والاعتداء على المعلومات الشخصية والمؤسساتية، والتشويه الرقمي، والابتزاز الإلكتروني، والقرصنة، والتلاعب بأنظمة الدفع الإلكتروني، وغيرها الكثير. وتعتبر الجرائم الإلكترونية عابرة للحدود، حيث يمكن للجاني أن يرتكب الجريمة من أي مكان في العالم ويستهدف ضحايا في بلدان أخرى، مما يزيد من تعقيد عملية التحقيق وملاحقة المرتكبين. وإثبات الجرائم الإلكترونية يمكن أن يكون صعبًا نظرًا لعدم وجود آثار مادية تدل على الجريمة وغياب الدليل المرئي القابل للقراءة بسهولة. وبالإضافة إلى ذلك، يستخدم المجرمون تقنيات تشفير وأدوات حماية تعيق جهود التحقيق وجمع الأدلة.

---

[٢٤] - **أحمد خليفة الملط، مرجع سابق، ص١٢١-١٢٣.**

لمكافحة الجرائم الإلكترونية، يجب تعزيز الوعي الأمني والتدريب، وتحسين الحماية الأمنية للأنظمة والبيانات، وتشديد القوانين وتطبيقها بفعالية، وتعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، وتعزيز التعاون بين القطاع العام والخاص والمؤسسات الأمنية والشركات التكنولوجية لتبادل المعلومات والخبرات. ويجب أيضًا تطوير التقنيات الأمنية وتحديثها بشكل منتظم للتصدي للتهديدات الجديدة والمتطورة، بالإضافة إلى إقامة فرق خبراء متخصصة في مجال مكافحة الجرائم الإلكترونية والتحقيق فيها. وعلى المستخدمين الالتزام بممارسات الأمان الرقمي، مثل استخدام كلمات مرور قوية وتحديث البرامج والتطبيقات بانتظام، وتجنب فتح رسائل البريد الإلكتروني المشبوهة أو الروابط غير المعروفة، وتثقيف الناس حول أنواع الاحتيال الإلكتروني المشتركة وكيفية التعامل معها.

المبحث الثاني

جرائم الأموال العامة الالكترونية للموظف العام

تمهيد وتقسيم:

تعتبر جرائم الإجرام الإلكتروني التي يرتكبها الموظف العام خلال أداء عمله الوظيفي من أكثر الجرائم الالكترونية تأثيرًا وتحديًا في العصر الحديث.

حيث يستفيد الموظف العام من الوصول المفتوح إلى مجموعة واسعة من المعلومات والبيانات الحساسة التي تخص المؤسسة التي يعمل فيها والأفراد الذين يتعاملون معها. ومن خلال هذا الوصول، يمكن للموظف العام أن يسلك طرقًا غير أخلاقية وغير قانونية للتلاعب بهذه المعلومات واستغلالها في أغراض شخصية أو غير قانونية.

ولقد خصصنا هذا المبحث لاستعراض الجرائم الالكترونية للموظف العام وقد إخترنا منها جرائم الأموال العامة وفقاً للتشريع المصري والإماراتي والكويتي، وذلك نقسم هذا المبحث إلى المطالب التالية:

- المطلب الأول: الموظف العام كجاني في المنظومة الالكترونية.
- المطلب الثاني: جرائم الأموال العامة في المنظومة الالكترونية.

المطلب الأول

الموظف العام كجاني في المنظومة الالكترونية

يعد التدخل البشري في المنظومة الإدارية الإلكترونية معياراً مهماً لتحديد مدى مسئولية الموظف العام في هذه المنظومة. تختلف نسبة التدخل البشري من عملية إلى أخرى في النظام الإلكتروني، حيث قد تتطلب بعض العمليات تدخلاً بشرياً كبيراً، بينما قد تتمتع عمليات أخرى بنسبة تدخل بشري أقل.

ومن أجل تحديد مدى مسئولية الموظف العام، ينبغي وضع شرح تحليلي للعمليات التي تتم عبر المنظومة الإدارية الإلكترونية. ومن المثالات التي يمكن أن نستخدمها هنا، نأخذ في الاعتبار إدارة الشؤون القانونية في منظمة حكومية.

وتعتمد إدارة الشؤون القانونية بشكل كبير على العمل الكتابي في المنظومة الإدارية الإلكترونية. يتمثل عمل الباحث القانوني في مكاتبة الجهات الأخرى المتعلقة بالمنظومة الإلكترونية، إعداد مذكرات قانونية لإبداء الرأي، إجراء تحقيقات، واتخاذ القرارات، وما إلى ذلك. تتطلب هذه العمليات الكتابية الكثير من التفاصيل والدقة في توثيق الإجراءات والمعلومات القانونية.

ومن ناحية أخرى، إدارة التفتيش المالي والإداري تعتمد على نوعين من العمليات في المنظومة الإدارية الإلكترونية. فالنمط الميداني يتضمن المعاينة الميدانية للأنشطة والعمليات، بينما يكون النمط الكتابي يتمثل في توثيق التقارير بعد المعاينة الميدانية.

وبالتالي، يجب التحدث وتوضيح العمليات الكتابية والعمليات الميدانية عبر المنظومة الإدارية الإلكترونية. وفي حالة العمليات الكتابية، يكون دور الموظف العام في إدارة الشؤون القانونية هو إعداد المذكرات القانونية وتوثيق البيانات والمعلومات ذات الصلة. يعتمد الموظف على النمط الكتابي للعمل في مراجعة الوثائق وتحليلها وإعداد التقارير القانونية وإبداء الرأي القانوني. أما في حالة العمليات الميدانية، فإدارة التفتيش المالي والإداري تتطلب التفاعل المباشر مع الميدان والقيام بمعاينات على الطبيعة. يتضمن ذلك زيارة المواقع، وتفقد السجلات والمستندات، وإجراء المقابلات والاستجوابات لجمع المعلومات والأدلة اللازمة. [٢٥]

لذلك، عند تحديد مدى مسئولية الموظف العام في المنظومة الإدارية الإلكترونية، يجب أخذ في الاعتبار نوعية العمليات المتعلقة بمهامه وصلاحياته في المؤسسة. وبناءً على

---

[٢٥]– صفاءة فتوح جمعة، الإطار القانوني والفني للتحول الرقمي في المنظمات الحكومية، دار الفكر والقانون، المنصورة، مصر، ٢٠٢٢، ص٦٠٢.

ذلك، يمكن تحديد مدى تأثيره ومسئوليته في العمليات الكتابية والعمليات الميدانية التي يقوم بها في المنظومة الإدارية الإلكترونية[٢٦].

أولاً- العمليات الكتابية عبر المنظومة الإدارية الالكترونية:

أ- في العمليات الكتابية النمطية، حيث يعتمد بعض الإدارات في المنظمات الحكومية على المكاتبات الرسمية لتنفيذ بعض المهام مثل استيفاء المستندات أو الاستفسارات. وتتم هذه المكاتبات بشكل نمطي وغالبًا ما يتم تدوينها وإرسالها بشكل آلي عبر المنظومة الإدارية الإلكترونية، وبالتالي فإن مسئولية الموظف العام في هذه الحالة تكون محدودة. يتم تنفيذ عملية التدوين والإرسال تلقائيًا بواسطة المنظومة الإلكترونية، وبالتالي فإن أي خطأ يحدث في التدوين أو ميعاد الإرسال يكون على عاتق مقدم الخدمة وليس على الموظف العام. وبالرغم من أن التدخل البشري في هذه العمليات محدود، إلا أنه يجب علينا أن نناقش المسئولية في إطار نظام التحكم الآلي بشكل أكثر تفصيلًا. يجب أن ننظر إلى مسئولية ثلاثة أطراف: المستخدم، والمبرمج، والمنتج.

- **مسئولية المستخدم:** يتحمل المستخدم المسئولية عن استخدام المنظومة الإلكترونية بشكل صحيح ومطابق للإجراءات المحددة. يجب أن يكون المستخدم على دراية بالسياسات والإرشادات المتعلقة بالعمليات الكتابية النمطية وأن يقوم بتنفيذها بدقة. [٢٧]
- **مسئولية المبرمج:** يقع على عاتق المبرمج مسئولية تطوير وبرمجة المنظومة الإدارية الإلكترونية بطريقة تضمن عملية التدوين والإرسال الآلي بشكل صحيح وموثوق. يجب على المبرمج ضمان عدم وجود أخطاء في البرمجة التي قد تؤثر على تنفيذ العمليات الكتابية النمطية بشكل سليم ومطابق للمعايير المطلوبة. يتحتم على المبرمج أيضًا توفير آليات للتحقق والتصحيح في حالة حدوث أي خطأ في عملية التدوين أو الإرسال.

---

(٢٦) – صفاء فتوح جمعة، مسئولية الموظف العام في إطار تطبيق نظام الادارة الالكترونية، دار الفكر والقانون، المنصورة، جمهورية مصر العربية، ٢٠١٤، ص٦٠٥.

(٢٧)– صفاءة فتوح جمعة، الإطار القانوني والفني للتحول الرقمي في المنظمات الحكومية، مرجع سابق، ص٦٠٢.

- **مسئولية المنتج:** يتوجب على الجهة الموردة للمنظومة الإدارية الإلكترونية أن تضمن جودة المنتج وأنه يستجيب بشكل صحيح وموثوق للعمليات الكتابية النمطية. يجب أن يتم توفير تحديثات وصيانة للمنتج بشكل منتظم لضمان سلامة وفعالية عمله.

وبالتالي نحن نرى، أن مسئولية الموظف العام في العمليات الكتابية النمطية في المنظومة الإدارية الإلكترونية محدودة، وأن التحكم الآلي يشمل مسئولية المستخدم والمبرمج والمنتج في توفير عملية التدوين والإرسال السليمة والموثوقة.

ففي حالة الموظف "ج" في المنظومة الإدارية الإلكترونية "ص" بإدارة الشؤون القانونية، إذا قام بإجراء مكاتبات بعد الوقت المحدد للإرسال وتسبب ذلك في صدور حكم قضائي يتسبب في خسائر للمنظمة الحكومية، يتوقف تحمل المسئولية على نسبة تدخل الموظف العام في العملية الإلكترونية المؤتمتة للإرسال.وإذا تم الإرسال تلقائياً بواسطة برنامج محدد دون تدخل من الموظف العام، وإذا كان الخلل الذي أدى إلى تأخير الإرسال يعود إلى خلل في البرنامج، فإن المسئولية تقع على المبرمج والمنتج، وليس على الموظف العام. في هذه الحالة، الموظف ليس مسؤولاً عن الخطأ الفني الذي تسبب في تأخير الإرسال والنتائج الناتجة عنه. ومع ذلك، إذا كان التوقيت لعملية الإرسال يعتمد على قرار من الموظف العام بدلًا من التوقيت التلقائي من البرنامج، في هذه الحالة يتحمل الموظف العام مسئولية كاملة. يكون لديه المسؤولية عن تحديد وتنفيذ الوقت الصحيح لإجراء المكاتبات وضمان أن يتم الإرسال في الوقت المناسب وفقًا للوائح والسياسات المعمول بها. وقد يتم تحميل الموظف العام والمبرمج بالمسئولية في حالات القوة القاهرة مثل انقطاع التيار الكهربائي أو عطل فني في المحطات أو كوارث طبيعية تؤثر على أداء المنظومة الإلكترونية. يتحمل المنتج المسئولية إذا كان الخطأ يعود إلى خلل في المنتج نفسه الذي قامت الشركة بتطويره وتوفيره[٢٨].

ونحن نرى، أن مسئولية الموظف العام تعتمد في العمليات الكتابية النمطية في المنظومة الإدارية الإلكترونية على درجة تدخله في هذه العمليات. وإذا كانت المنظومة مؤتمتة

---

[٢٨] – صفاء فتوح جمعة، الإطار القانوني والفني للتحول الرقمي في المنظمات الحكومية، مرجع سابق، ص٦٠٨.

بشكل كامل وتتم عملية التدوين والإرسال تلقائياً بدون تدخل من الموظف العام، فإن المسئولية تكون محدودة لدى المبرمج والمنتج.

ومع ذلك، إذا كان هناك تدخل من الموظف العام في عملية التدوين والإرسال، فإن المسئولية قد تتحمل بشكل كامل من قبل الموظف، خاصة إذا كان الخطأ ينجم عن قرارات أو إجراءات غير صحيحة أو تأخير في الإرسال ناتج عن تقصير أو إهمال من الموظف العام.

وفي الحالات التي يتدخل فيها عوامل خارجة عن سيطرة الموظف العام وتؤثر على عملية التدوين والإرسال، مثل القوة القاهرة أو أعطال فنية، قد يتقاسم المسئولية بين الموظف والمبرمج والمنتج، حسب نوع الخلل وسببه.

لذلك، يجب إجراء تحليل فني دقيق لتحديد مدى التدخل البشري في العمليات الكتابية النمطية ومدى المسئولية المترتبة على الموظف العام والمبرمج والمنتج في حالة وقوع أي خطأ أو ضرر. وهذا التحليل يساعد على تحديد المسئولية المناسبة واتخاذ الإجراءات اللازمة لتلافي حدوث مشكلات مستقبلية وتحسين أداء المنظومة الإدارية الإلكترونية.

ب-العمليات الكتابية الغير نمطية:

تتواجد أيضاً العمليات الكتابية الغير نمطية في منظومة الإدارة الإلكترونية، حيث يحتاج بعض أعمال الإدارة إلى تكوين وصياغة وثائق غير قابلة للتوحيد والتنسيق بشكل تلقائي. في هذه الحالة، يقوم الموظف العام بصياغة هذه الوثائق بنفسه ويتولى الضغط على زر الإرسال. وبالتالي، تكون المسئولية الكاملة في هذه العمليات على الموظف العام نظراً لأن العملية تمت بتدخل بشري كبير رغم أن هناك نصف أتمتة مطبقة. ومع ذلك، إذا كانت الأخطاء التي تسببت في الضرر يمكن أن تعزى إلى عطل فني في البرنامج نفسه أو إلى مقدم الخدمة، فإن المسئولية قد تتحمل جزئياً أو كلياً من قبل المبرمج أو المنتج.

ويجب أن يتم إجراء تحليل دقيق للعمليات الكتابية الغير نمطية وتحديد مسئولية كل طرف في حالة حدوث أخطاء أو ضرر. يجب أن يتم توفير آليات لمراقبة ومراجعة هذه العمليات وضمان تدابير الجودة والتحقق اللازمة للحد من حدوث الأخطاء وتقليل المسئولية. [٢٩]

---

[٢٩] – صفاء فتوح جمعة، الإطار القانوني والفني للتحول الرقمي في المنظمات الحكومية، مرجع سابق، ص٦٠٧.

ونحن نرى، يتوجب على الموظف العام أن يكون حذراً ومسؤولًا في أداء واجباته في العمليات الكتابية الغير نمطية، ويجب عليه التأكد من صحة ودقة المعلومات والوثائق قبل الضغط على زر الإرسال، والالتزام بالسياسات والإرشادات المعمول بها.

ثانياً-العمليات الميدانية عبر المنظومة الإدارية الالكترونية:

تشمل المنظومة الإدارية الإلكترونية أيضًا العمليات الميدانية التي تتطلب معاينة على الطبيعة للمؤسسات والمنشآت الحكومية وغير الحكومية. وعلى الرغم من أن العمليات الميدانية قد تأثرت بوسائل الاتصال التكنولوجية، إلا أن بعضها يمكن تنفيذه عبر شبكة المنظومة الإدارية الإلكترونية، بينما البعض الآخر لا يمكن إنجازه عبر هذه الشبكة، وسوف نوضح ذلك فيما يلي:

- **العمليات الميدانية التي يمكن إنجازها عبر التقنيات التكنولوجية،** تتعلق بأعمال المتابعة لتنفيذ مشاريع معينة أو تكليفات قيادية. يتم استخدام الشبكة الإلكترونية للمعلومات لفحص وتدقيق ومتابعة وتنسيق بين الجهات المعنية بهذه العمليات، مما يسهم في تحسين فعالية الرقابة وتنفيذ الأعمال بشكل سلس وفعال.
- **أما العمليات الميدانية التي لا يمكن إنجازها عبر التقنيات التكنولوجية،** فتتعلق بأعمال التفتيش على المؤسسات الحكومية والتجارية ومراقبة الامتثال لقرارات الوزارة وغيرها. تعتبر هذه العمليات الميدانية أكثر تأثيراً على فعالية الرقابة، حيث يكون التفتيش والمراقبة في موقع الحدث ويتطلب تواجد الفريق المختص بشكل مباشر.

ونحن نرى، أن مسئولية الموظف العام في العمليات الميدانية، سواء كانت على الطبيعة أو عبر المنظومة الإدارية الإلكترونية، تعتمد بالطبع على مدى التدخل البشري. يتم تحديد ذلك من خلال التقرير الفني للعملية الإلكترونية، حيث يقوم التقرير بتحديد نسبة الخطأ المرتبط بالموظف ونسبة الخطأ الفني الغير مرتبط بالموظف العام، وهذا يؤثر على مدى مسئولية الموظف العام. وإذا كان التقرير الفني يشير إلى أن الخطأ يرجع إلى الخطأ المرتبط بالموظف العام، فإن المسئولية تقع على عاتقه بشكل كامل. ومن الجدير بالذكر أن الموظف العام يجب أن يتمتع بالمهارات والمعرفة اللازمة لتنفيذ العمليات الميدانية بكفاءة ودقة. ومن جانب آخر، إذا كان الخطأ الناجم عن عيب فني في المنظومة الإدارية

الإلكترونية وغير مرتبط بالموظف العام، فإن المسئولية قد تكون للمبرمج أو المنتج. ويجب على المبرمجين والمطورين ضمان تصميم وبرمجة نظام قوي وموثوق يتجنب الأخطاء التقنية التي يمكن أن تتسبب في أضرار للمنظمة الحكومية. وبالنهاية يمكننا القول أن إدارة العمليات الميدانية تتطلب الكفاءة والمهارة من الموظفين العامين وضمان توفر الأدوات التكنولوجية اللازمة لتنفيذ المهام بنجاح. يجب توفير التدريب والدعم المستمر للموظفين للتأكد من قدرتهم على التعامل مع المنظومة الإدارية الإلكترونية بكفاءة وتحمل المسئولية المناسبة.

ثالثاً- الموظف الروبت في المنظومة الإدارية الالكترونية:

عرف المشرع الكويتي في نص المادة (١) من قانون القانون رقم (٦٣) لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات النظام الإلكتروني المؤتمت بأنه " برنامج أو نظام إلكتروني لحاسب آلي تم إعداده ليتصرف أو يستجيب لتصرف بشكل مستقل، كليا أو جزئيا، دون تدخل أو إشراف أي شخص طبيعي في الوقت الذي يتم فيه التصرف أو الإستجابة له".[٣٠]

ونحن نرى، من خلال هذا التعريف الذي وضعه المشرع الكويتي للنظام الإلكتروني المؤتمت اهتمامه الشديد بتحديد طبيعة النظام الذي يعمل بشكل مستقل وبدون تدخل بشري. وهذا التعريف يساعد في تحديد نطاق المسؤولية المتعلقة بالأخطاء الإلكترونية التي يرتكبها النظام المؤتمت. وبالمقابل، قد يكون التعريف غير مفصل في التشريعات المصرية والإماراتية، مما قد يتسبب في ضبابية أو تأويلات في فهم طبيعة النظام المؤتمت ومدى تحمله المسؤولية عن الأخطاء الإلكترونية. وبناءً على ذلك، **يمكن القول إن المشرع الكويتي** قد أحسن في وضع تعريف واضح ومفصل للنظام الإلكتروني المؤتمت، مما يعزز الشفافية ويسهم في تحديد المسؤولية عن الأخطاء الإلكترونية التي يتسبب فيها النظام المؤتمت.

بينما نجد أن المشرع الإماراتي وضع تعريفاً للربوت الإلكتروني في القانون رقم (٣٤) لسنة ٢٠٢١ من قانون مكافحة الشائعات والجرائم الإلكترونية، حيث عرف بأنه "برنامج إلكتروني يتم إنشاؤه أو تعديله لغرض تشغيل المهام

---

[٣٠] - **المادة (١) من القانون رقم (٦٣) لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات الكويتي.**

المؤتمتة بكفاءة وسرعة".[٣١] **ونحن نرى،** أن المشرع الإماراتي أحسن في وضع تعريفاً للربوت الإلكتروني، بينما أغفل عنه المشرع المصري والكويتي.

ونحن نرى، من الضروري أن يكون لدينا تعاريف واضحة ومحددة للمصطلحات القانونية المستخدمة في مجال التكنولوجيا الحديثة، بما في ذلك الربوت الإلكتروني، لأن هذا يساهم في تحقيق الشفافية وفهم القواعد القانونية المتعلقة بالاستخدام والمسؤولية المتعلقة بالربوتات الإلكترونية.

ولو نظرنا إلى الموظف الروبوت في المنظومة الإدارية الالكترونية فإنه يختلف قليلاً عن الموظف العام التقليدي. ووفقًا للمعايير المعتادة لتعيين الموظف العام، يجب أن يتوفر له ثلاثة معايير: التعيين من قبل السلطة المختصة، القيام بعمل دائم، والخدمة في مرفق عام.

ومع ذلك، في حالة الموظف الروبوت، قد يكون هناك تحدي في تطبيق المعيار الأول، وهو التعيين من قبل السلطة المختصة. حيث أن الموظف الروبوت لا يتم تعيينه في المعنى التقليدي، بل يتم برمجته وتشغيله بواسطة فريق تقني. ومع ذلك، يجب أن يتم توجيه الموظف الروبوت وتحديد المهام التي يقوم بها وفقًا لمتطلبات المؤسسة الحكومية.

بالنسبة للمعايير الأخرى، فإن الموظف الروبوت يمكن أن يتوافق معها. فهو يقوم بعمل دائم، حيث يمكن أن يعمل على مدار الساعة دون توقف وفقًا للبرمجة المحددة. كما يمكن أن يخدم في مرفق عام، حيث يتعامل مع المعاملات الحكومية ويقدم الخدمات اللازمة للمواطنين[٣٢].

ونحن نرى، يجب على المؤسسات الحكومية التأكد من تطبيق القوانين والأنظمة اللازمة لضمان تحقيق الموظف الروبوت للمعايير المطلوبة. ومع ذلك، ينبغي أيضًا دراسة

---

[٣١] - المادة (١) من القانون رقم (٣٤) لسنة ٢٠٢١ في مكافحة الشائعات والجرائم الإلكترونية لدولة الإمارات العربية المتحدة.

[32]– John O'Reilly, Day Pitney LLP, Criminal Liability of Companies Survey, http://www.lexmundi.com/images/lexmundi/PDF/BusinessCrimes/CrimLiabilityUSANew'/o20Jersey.pdf (last visited May 19, 2010).

- **Brożek, B., & Jakubiec, M. (2017). On the legal responsibility of autonomous machines. Artificial Intelligence and Law, 25(3), 293-304. https://doi.org/10.1007/s10506-017-9207-8.**

الجوانب القانونية والأخلاقية المتعلقة بتوظيف الموظف الروبوت في العمل الحكومي، وضمان أن يتم استخدامه بطرق تلبي متطلبات العدالة والشفافية وحقوق المواطنين.

الخلاصة: أن المسئولية في المنظومة الإدارية الالكترونية تتأثر بنسبة التدخل البشري واستخدام التقنيات التكنولوجية. ففي العمليات الكتابية النمطية، المسئولية تتقسم بين الموظف العام والمبرمج والمنتج. وفي العمليات الكتابية الغير نمطية، المسئولية تكون للموظف العام بشكل كامل، مع استثناءات للأخطاء التقنية غير المرتبطة بالموظف العام.

وفي العمليات الميدانية، المسئولية تتأثر بمدى استخدام التقنيات التكنولوجية. والعمليات التي يمكن إنجازها عبر التقنيات التكنولوجية تتقاسم المسئولية بين الموظف العام والمبرمج والمنتج. أما العمليات التي لا يمكن إنجازها عبر التقنيات التكنولوجية، فالمسئولية تكون للموظف العام بشكل كامل. ويجب توفير التدريب والدعم المستمر للموظفين العامين لضمان قدرتهم على التعامل مع المنظومة الإدارية الالكترونية وتحمل المسئولية الملائمة. كما يجب أن تراعى المؤسسات الحكومية الجوانب القانونية والأخلاقية في توظيف التقنيات الحديثة في العمل الحكومي.

المطلب الثاني

جرائم الأموال العامة في الإدارة الالكترونية

عرف المال في اللغة بأنه "هو ما ملكته من جميع الأشياء، وجمعه وأموال، وكان في الأصل ما يملك من الذهب والفضة، ثم أطلق على كل ما يقتنى، ويملك من الأعيان، أكثر ما يطلق عند العرب على الإبل؛ لأنها كانت أكثر أموالهم". (٣٣) وعرفه البعض بأنه " كل ما يمكن حيازته، وإحرازه، والإنتفاع به في العادة سواء أكان محرزاً، ومنتفعاً به فعلاً، كجميع الأشياء التي تملكها من الأرض، أو متاع، أو حيوان، أو نقود، أم غير محاز، ولا ينتفع به،

(٣٣) – ابن منظور، أبو الفضل جمال الدين محمد بن مكرم، لسان العرب، دار صادر، بيروت، ٢٠١٠، ص٢٤٠.

ولكن من الممكن أن يتحقق فيه ذلك، كجميع المباحث من الأعيان، مثل الأسماك في البحر، والطير في الجو، والشجر في الغابات، إذ من الممكن أن يحاز كل ذلك، وينتفع به". [١]

بينما عرف المال العام بأنه "هو جميع الأموال المملوكة للدولة أو لغيرها من الأشخاص العامة، محلية، أو مرفقية، وسواء أكانت هذه الأموال عقارات، أم منقولات، وعلى ذلك تعتبر جميع الأموال المملوكة للأشخاص العامة أموالاً عامة أي كان نوع تخصيصها، أي سواء أكانت مخصصة لاداء منفعة إدارية، أم إقتصادية، أم غيرها، من أوجه النفع العام".[٢] كما عرفت الأموال العامة بأنها" الأموال التي تخصص لخدمة المرفق العام أو لخدمة الجمهور مباشرة".[٣] مباشرة".[٣]

وفي نظرة العديد من القوانين الوضعية نجد أنها تركز في تعريفها للمال العام على عناصر أهمها:

- كون المال عائداً للدولة أو للأشخاص المعنوية العامة التابعة للدولة لكي يعد مالاً عاماً.
- إضافة إلى اشتراط أن يخصص ذلك المال للمنفعة العامة كقاعدة عامة.

ويضيف البعض ضرورة أن يكون المال مادياً واستبعاد كل ما هو معنوي لصعوبة تخصيصه، ولكني لا اتفق مع هذا الشرط حيث ممكن أن يكون المال العام معنوياً مثل المعلومات والبرامج، النظام المعلوماتي، والمستندات الالكترونية الموجودة على أجهزة الحواسيب الآلية للموظفين في المنظمات الحكومية.

أولاً- التعريف بجرائم الأموال العامة

تعتبر الجريمة من المشاكل القديمة التي ظهرت في البشرية منذ الأزل، وتم ذكرها في العديد من الأديان والشرائع والأعراف والقوانين. وتعد مشكلة السلوك الإجرامي واحدة من أخطر وأعقد المشاكل التي تواجهها المجتمعات الحديثة. لكن ذلك لا يعني أنها مشكلة حصرية للمجتمعات المعاصرة فحسب، بل إنها تعود إلى فترات زمنية سابقة وتواجه المجتمعات في كل عصر. فعندما ينشأ مجتمع جديد، يظهر فيه التصرف الجرمي بأشكال مختلفة. وتتنوع

---

(١) – محمد عبد الفتاح الأمير، الوسيط في جرائم العدوان على المال العام، المجموعة العلمية للطبع والنشر، القاهرة، ٢٠٢١، ص٢٨.

(٢) – رفيق محمد سلام، الحماية الجنائية للمال العام، دار النهضة العربية، القاهرة، ٢٠١٨، ص١٣١.

(٣) – محمود أحمد سليمان البراشدي، النظام القانوني لأموال المرافق في ظل سياسة الخصخصة، دار النهضة العربية، القاهرة، ٢٠١٧، ص١٠٩.

أشكال الجريمة من تلك التي ترتكب في المجال الاقتصادي والمالي إلى تلك المتعلقة بالعنف والجرائم العنصرية والجرائم الجنسية وغيرها. وبالتالي، يمكن القول إن الجريمة ليست مشكلة حديثة فحسب، بل إنها تواجه المجتمعات في جميع العصور. [١]

حيث تعتبر الجريمة سرطان اجتماعي يتغذى من العوامل الاجتماعية والاقتصادية والنفسية. وفي معظم التشريعات، يتفق القانون على أن الجريمة تشمل أعمالًا مخالفة للقانون، سواء كان ذلك بارتكاب فعل محظور قانونيًا أو عدم القيام بفعل مطلوب بموجب القانون. وبناءً على ذلك، يمكن اعتبار الجريمة كسلوك بشري يتضمن الإرادة والتصرف، سواء كان هذا التصرف إيجابيًا أو سلبيًا، ويتوافق مع النص القانوني المحظور أو المطلوب. ويجب أن تتوفر الأسباب الكافية لحدوث النتيجة الجرمية المرتبطة بهذا السلوك[٢].

ويشتق مصطلح "الجريمة" من الفعل "جرم"، ويتعلق بمعانٍ متعددة تشمل الكسب غير المستحسن، والذنب، والقطع[٣]. تستخدم هذه الكلمة للإشارة إلى فعل المجرم الذي يكسب من خلاله ما لا يحق له ويقتطع حقًا معينًا، وبالتالي يقطع الأمن عن نفسه وعن الآخرين، وتستدعي تلك الأفعال عقوبة. [٤].

ونحن نرى، أن الجريمة في اللغة العربية تعني أن الفاعل قام بفعل يتضمن كسبًا غير مشروع، وأثمًا، وانتهاكًا للأمن، وعندئذٍ يستحق العقاب.

أما في الفقه الجنائي، يتم تعريف الجريمة على أنها "كل عمل أو امتناع ضار، له مظهر خارجي، ليس استعمالًا لحق ولا قيامًا بواجب، يحرمه القانون ويفرض له عقابًا، يقوم به إنسان لتحمل المسؤولية الجنائية". [٥]

ونحن نرى، أن هذا التعريف يشمل جوانب مختلفة للجريمة، بما في ذلك العمل أو الامتناع، والأثر الضار، والتعارض مع القانون، ووجوب تحمل المسؤولية الجنائية.

---

[١] – محمد علي سويلم، السياسة الجنائية في مكافحة جرائم المال العام، المصرية للنشر والتوزيع، القاهرة، ٢٠١٩، ص٥٤.

[٢] – إبراهيم خليفة، الجريمة والعقاب، أكاديمة نابف العربية للعلوم الأمنية، الرياض، ٢٠٠٨، ص٦٤.

[٣] – ابن منظور، مرجع سابق، ، ص٢٤٠.

[٤] – محمد أبوزهرة، الجريمة، دار الفكر العربي، القاهرة، ١٩٩٨، ص ١٩.

[٥] – محمد محي الدين عوض، القانون الجنائي، مبادئه الأساسية ونظرياته العامة، مطبعة جامعة القاهرة، القاهرة، ٢٠١٢، ص٩٥.

ولو نظرنا إلى تعريف المال، فيتم تعريفه في اللغة بأنه "ما يملكه الشخص من جميع الأشياء والثروات، ويشمل الأموال والأعيان والممتلكات". (١) (١)،

ونحن نرى، أن هذا التعريف يشمل الأموال والأعيان والممتلكات التي يمتلكها الشخص. حيث يمثل المال يمثل القيمة الاقتصادية والثروة التي يستخدمها الأفراد والمؤسسات في التبادل التجاري وتلبية الاحتياجات والرغبات. ويمكن أن يشمل المال العملات النقدية، والحسابات المصرفية، والأسهم والأسواق المالية، والعقارات، والمركبات، والممتلكات الثقافية وغيرها.

---

(١) – **رفيق محمد سلام، الحماية الجنائية للمال العام، دار النهضة العربية، القاهرة، ٢٠١٨، ص١٣١.**

(١) المال لغة: من المول وأصله مال يمول مولا، ومؤولا، أي أكثر ماله ويجمع على أموال وهو ما يملكه الإنسان من كل شيء، في اصطلاح الفقهاء: اختلف تعريف الفقهاء للمال تبعا لاختلافهم في أحكامه على اصطلاحين رئيسيين هما اصطلاح الحنفية واصطلاح الجمهور.

١- اصطلاح الحنفية: عرف المتقدمون من فقهاء المذهب الحنفي المال بتعريفات كثيرة وهي وإن اختلفت في ألفاظها إلا أنها تتفق في معناها ومرماها، وأوضحها تعريفه بأنه عين يجري فيه التنافس والابتذال أي بذل العوض وبهذا المعنى لا يعتبر الشيء مالا وفقا للإصلاح الحنفي إلا إذا توفر فيه عنصران:

العنصر الأول: العينية بأن يكون الشيء ماديا له وجود خارجي ذلك أن العين يراد منها الشيء المادي الذي له مادة ويتأتى إحرازه وحيازته.

العنصر الثاني: التمول: يقصد بالتمول التنافس وبذل العوض وذلك بأن تجري عادة الناس كلا أو بعضا على التنافس على هذه العين وحيازتها وفي سبيل الحصول عليها يهون عليهم بدل أموالهم، فإذا كان الشيء لا يجري عليه التنافس بين الناس ولا يبذلون فيه أموالهم لا يكون مالا.

٢- اصطلاح الجمهور: عرف جمهور الفقهاء ومنهم الشافعية والحنابلة والمالكية المال بعدة تعريفات يؤخذ منها أن المال يطلق على كل ماله قيمة مادية بين الناس وأجاز الشارع الانتفاع به في حاله السعة والاختيار وينضح لنا أن مالية الأشياء في اصطلاح جمهور الفقهاء، أن الشيء لا يكون مالا إلا إذا توفر له عنصران.

العنصر الأول: أن يكون الشيء له قيمة بين الناس سواء كان عينا أو منفعة ماديا أو معنويا. فلو كان الشيء تافها لا قيمة له بين الناس، لا يكون مالا عينا أو منفعة كحبة قمح.

العنصر الثاني: أن يكون الشيء قد أباح الإسلام الانتفاع به في حالة السعة والاختيار كالحبوب والإبل والعقارات، أما إذا كان الإسلام حرم الانتفاع به كالخمر والخنزير ولحم الميتة فإنه لا يكون مالا، وبالمقارنة بين اصطلاحي الحنفية وجمهور الفقهاء يظهر مدى بينهما من اختلاف في مالية الأشياء، ذلك أن الحنفية لا يعتبرون المنافع أموالا كما أنهم يعتبرون الخمر والخنزير ونحوهما مما يتعامل فيه غير المسلمين من أهل الذمة أموالا.

بين يذهب جمهور الفقهاء إلى أن المنافع أموال لأن مصادرها وهي الأعيان يجري عليها الإحراز والحيازة ولم يعتبر الجمهور الخمر والخنزير أموالا بالنسبة لمسلم ولا بالنسبة لغيرهم، لعدم إباحة الإسلام الانتفاع بهما.

هذا وإن كان متقدموا الحنفية يرون أن العينية إحدى عنصري المالية فإن متأخريهم قد أطلقوا المال على الأعيان والمنافع وعلى كل ماله قيمة نقدية وعلى ذلك فلا تتطلب المالية للأشياء، سوى إمكان تقديرها بالنقد أي أن الشيء إذا كان له قيمة فإنه يكون مالا.

وابتناء مالية الشيء على القيمة وفقا لهذا الإطلاق سوف يسمح بتوسيع دائرة الأموال، وبخاصة في هذا العصر الذي اتسم بالتطور العلمي والحضاري، ليشمل أشياء لم تكن معروفة من قبل مادام يمكن تقديرها بالنقود ومن ذلك الأشياء المعنوية فيما يعرف بالحقوق الذهنية أو حقوق الابتكار، انظر ***أ/ يدعلي محي الدين القره داغي*** المقدمة في المال والاقتصاد والملكية والعقد الطبعة الأولى ١٤٢٧ هـ ٢٠٠٦م، ص ١١١، ***أ/حمد فرج حسين*** "الملكية ونظرية العقد في الشريعة الإسلامية" الدار الجامعية ١٩٨٦، ص. ٩، ١٠، للمزيد من المعلومات راجع " مفهوم المال وتقسيماته" على الموقع الالكتروني:
https://www.bibliotdroit.com/2018/07/blog-post_6.html

وهناك تعريف آخر للمال يشير إلى أنه "كل ما يمكن حيازته واحتياطه والاستفادة منه بشكل عام، سواء كان مملوكًا بالفعل ومستفادًا منه فعليًا، مثل الأموال والممتلكات والممتلكات الثقافية، أو غير مملوك ولكن يمكن تحقيقه والاستفادة منه في بعض الأحيان، مثل الأسماك في البحر والطيور في الجو والأشجار في الغابات".[1]

ونحن نرى، أن هذا التعريف للمال يشمل الأموال الفعلية التي يمتلكها الفرد بالفعل ويستفيد منها، بالإضافة إلى الممتلكات التي ليست مملوكة حاليًا ولكن يمكن الحصول عليها والاستفادة منها في بعض الحالات.

كما يعرف القانون "المال العام" بشكله المألوف باعتباره مالا ماديا له قيمة مالية، فيتوجب على الموظف المحافظة عليه، وعدم الإضرار به، أو استخدامه لمصلحة شخصية.

وأحدثت المنظومة الإلكترونية تحولًا في جرائم الأموال العامة، حيث يتم استهداف المعلومات كوسيلة لارتكاب الجرائم المالية. ويمكن أن تكون جريمة الاختلاس والاستيلاء على المعلومات أحد أشكال هذه الجرائم، حيث يتم سرقة أو استغلال المعلومات الحكومية للحصول على مكاسب غير قانونية. كما يمكن أن تتعلق جريمة الإضرار بالمعلومات بالمعلومات الحكومية، حيث يتم التلاعب أو التدخل في تلك المعلومات بهدف تشويش العملية الحكومية أو تسبب أضرار مالية أو سمعة سيئة للجهات الحكومية. بإضافة إلى ذلك، يمكن أن تكون الرشوة معلوماتية، حيث يتم تبادل المعلومات الحكومية بطرق غير قانونية أو تسريبها بهدف الحصول على رشاوى أو تحقيق مكاسب غير قانونية. وسوف نوضح ذلك فيما يلي:

وتمثل مخرجات الحاسوب قيمة اقتصادية قابلة للحيازة والنقل وتكون محلا للحقوق المالية، سواء أكانت في صورة معلومات ، أو مستندات إلكترونية، أو مستندات ورقية، وتخضع للحماية القانونية المقررة للأموال العامة المنقولة والعائدة للجهات الحكومية، ومن ثم يتوجب على الموظف الالتزام بالمحافظة عليها شأنها في ذلك شأن سائر الأموال العامة الأخرى ذات الصفة المادية، فيجب على الموظف العام عدم الإضرار بمخرجات النظام الوظيفي الإلكتروني من مستندات " إلكترونية، ورقية" ومعلومات و بيانات وما في حكمها، فالمعلومات والبيانات وكافة المستندات الموجود على النظام الوظيفي الإلكتروني يعد مالا عاما معنويا.

وبناء عليه، فإن مخرجات المنظومة الادارية الالكترونية " "ESEDEEGSP" تعد مالا عاما ممكن أن تكون محلا لجرائم الأموال العامة، وبالتالي نجد أن التحول الرقمي قد أضاف نوعا

---

[1] – **محمود أحمد سليمان البراشدي، النظام القانوني لأموال المرافق في ظل سياسة الخصخصة، دار النهضة العربية، القاهرة، ٢٠١٧، ص١٠٩.**

جديداً من جرائم الاموال العامة، ألا وهي جرائم الموال العامة المعلوماتية " فيمكن أن يكون هناك جرائم استيلاء معلوماتية، ووجرائم اختلاس مستندية إلكترونية، ولكن السؤال الذي يفرض نفسه على بساط البحث، هل هذا النوع الجديد من جرائم الأموال العامة لها نظامها الخاص التي تتميز به عن جرائم الأموال العامة بصفة عامة؟

ففي الواقع، إن التحول الرقمي لا يفرض نوعا جديدا من الجرائم له نظامه الخاص، فهذه النوعية الجديدة من الجرائم تخضع للنظام العام لجرائم الأموال العامة، إلا أنها مختلفة في محلها، وطرق إثباتها التي تعتمد على النواحي الفنية أكثر من النواحي القانونية، وطبيعة الدليل الذي يثبت الجريمة والتي يتميز بالخفاء أكثر من الثبات، .

ثانياً – أشكال وصور جرائم المال العام،:

تتعدد أشكال وصور جرائم المال العام منها .

١– جريمة الاختلاس وجريمة الاستيلاء على الأموال والجرائم الملحقة بها:

جريمة الاختلاس وجريمة الاستيلاء على الأموال تشتركان في الجانب العام الذي يتعلق بالاستيلاء غير المشروع على الممتلكات أو الأموال، ولكنهما تختلفان في بعض الجوانب. جريمة الاختلاس تتطلب وجود عنصرين أساسيين وهما العنصر المادي والعنصر النفسي، حيث يقوم

الفاعل بالاستيلاء على المال الذي يكون تحت حيازته أو سلطته بسبب وظيفته أو مهمته، ويقوم بذلك بخرق واجبه في المحافظة على نزاهة الوظيفة. أما جريمة الاستيلاء على الأموال، فلا تشترط وجود مال موجود بين يدي الجاني بسبب وظيفته، بل يمكن أن تشمل أموالًا تعود للدولة أو لأفراد آخرين [١].

وعلى الرغم من أوجه الشبه بين الجريمتين، إلا أنهما تختلفان في بعض النقاط. تتطلب جريمة الاختلاس وجود المال المستولى عليه موجوداً بين يدي الجاني بسبب وظيفته أو مهمته، بينما جريمة الاستيلاء على الأموال لا تشترط ذلك. كما أن جريمة الاختلاس تعتبر من

---

[١] – **صفاء فتوح جمعة، الإطار القانوني والفني للتحول الرقمي في المنظمات الحكومية، مرجع سابق، ص٦١٩.**

الجرائم المخلة بواجبات الوظيفة، في حين أن جريمة الاستيلاء على الأموال لا تقتصر على الوظيفة فقط. ويجب أن يتوفر في كلتا الجريمتين العنصر العمدي، وأن يكون الجاني يعلم بالقصد الجنائي لفعله. ويعدان كلتا الجريمتين من الجنايات وتحتاجان إلى توافر العلم والإرادة لثبوت القصد الجنائي فيهما. [١]

وقد أضافت المنظومة الادارية الالكترونية نوعا جديدا من جرائم الأموال العامة، فهذه المنظومة أنشأت جرائم استيلاء معلوماتية، وجرائم إختلاس معلوماتية، حيث أصبحت الأموال العامة لم تقتصر على الأموال المادية، ولمن هناك أموال عامة معنوية " وهي المعلومات، البرامج، الانظمة المعلوماتية، المستندات الإلكترونية، .....وغيرها من مكونات المنظومة الادارية الالكترونية" ، وهذه الجرائم الجديد من الأموال العامة لا تخرج عن القواعد العامة لهذه الجرائم، فجرائم الاستيلاء والاختلاس المعلوماتي لا يخرج إطارها عن إطار القواعد العامة لجرائم الاستيلاء والاختلاس إلا من حيث محل الجريمة.

كما يمكن أن تشمل الجرائم المحلقة بها الرشوة المعلوماتية، حيث يتم تبادل المعلومات الحكومية بصورة غير قانونية أو تسريبها بهدف الحصول على مكاسب غير قانونية. كما يمكن أن تشمل الجرائم المحلقة بها أيضاً جرائم الإضرار بالمعلومات الحكومية، حيث يتم التلاعب أو التدخل في تلك المعلومات بهدف تشويش العملية الحكومية أو تسبب أضرار مادية أو سمعة سيئة للجهات الحكومية.

٢- جريمة أضرار الموظف بالأموال والمصالح العامة:

جريمة أضرار الموظف بالأموال والمصالح العامة تتمثل في استغلال الموظف العمومي لوظيفته العامة بهدف تسبب الضرر في المصالح العامة التي يكلف بحمايتها، سواءً للحصول على مصلحة شخصية لنفسه أو لأطراف أخرى. يمكن تقسيم هذه الجريمة إلى صورتين، إضرار عمدي بالأموال وإضرار غير عمدي بالأموال. يكمن الجانب المادي للجريمة في تسبب الضرر بصورة متعمدة في حالة الإضرار العمدي، وبصورة غير متعمدة في حالة الإضرار غير العمدي.[٢]

---

[١] - سهير عبد المنعم، الحماية الجنائية لنزاهة الوظيفة العامة، دار النهضة العربية، القاهرة، ٢٠١٦، ص ٣٠٣.

[٢] - محمد أنور حماد، الحماية الجنائية للأموال العامة، دار الفكر الجامعي، الإسكندرية، ٢٠٢٠، ص٣٤.

وهناك أمثلة على جرائم اضرار الموظف بالأموال والمصالح العامة في المنظومة الإدارية الالكترونية:

- التلاعب في المعلومات أو البيانات الحكومية بهدف تغييرها أو تشويهها أو تدليسها للتسبب في خسائر مالية أو تأثير سلبي على مصالح الجهة الحكومية.
- سوء استخدام السلطة المخولة للموظف العام بغرض تحقيق مكاسب شخصية غير قانونية على حساب المصالح العامة، مثل قبول رشاوى أو المشاركة في أعمال فساد.
- التسبب في تلف أو تعطيل الأنظمة الإلكترونية المتعلقة بالمنظومة الإدارية الالكترونية، سواء بشكل متعمد أو بالإهمال، مما يتسبب في توقف العمليات الحكومية وتكبد خسائر مالية وتأخير في تقديم الخدمات.

وفي سياق ذلك قالت محكمة نقض أبو ظبي: لما كانت المادة (٢٦٠) من قانون الجرائم والعقوبات الإتحادي إذ نصت على أنه يعاقب بالسجن المؤقت كل موظف عام، أو مكلف بخدمة عامة استغل وظيفته فاستولى بغير حق على مال للدولة، أو لإحدى الجهات التي ورد ذكرها في المادة الخامسة أو سهل ذلك لغيره، فقد دلت في صريح عباراتها وواضح دلالاتها على أن جريمة الاستيلاء على مال الدولة بغير حق تقتضي وجود المال في ملك الدولة عنصراً من عناصر ذمتها المالية، ثم قيام موظف عام أو من في حكمه أياً كان بانتزاعه منها خلسة أو حيلة أو عنوة بنية تملكه أو تضييعه على صاحبه ولا يعتبر المال قد دخل في ملك الدولة إلا إذا كان قد آل إليها بسبب صحيح ناقل للملك وتسلمه من الغير موظف مختص بتسلمه على مقتضى وظيفته."

ونحن نرى، أن جريمة اضرار الموظف بالأموال والمصالح العامة في المنظومة الإدارية الالكترونية تتعلق بتعمد أو إهمال الموظف العام في إلحاق ضرر بالأموال والمصالح العامة المتعلقة بالمنظومة. ويشمل ذلك التلاعب في المعلومات والبيانات الحكومية، واستغلال السلطة لتحقيق مكاسب شخصية غير قانونية، وتعطيل أو تلف الأنظمة الإلكترونية المرتبطة بالمنظومة. تعد هذه الجريمة جزءاً من قوانين الجنح الجنائية وتخضع للتشريعات المعمول بها في كل بلد بما في ذلك التشريعات المصرية والكويتية والإماراتية. يهدف القانون إلى محاسبة

الموظف العام المسؤول وتطبيق العقوبات المناسبة لهذه الجريمة.

وبشكل عام محتويات المنظومة الادارية اللالكترونية " ESEDEEGSP" من معلومات وبرامج ومستندات إلكترونية وغيرها أموال ومصالح عامة يعتبر الاضرار بها عمدا أو بإهمال من قبل الموظف العام" جريمة اضرار الموظف بالاموال والمصالح العامة المعلوماتية " لا تختلف عن القواعد العامة لهذه الجريمة في القانون الجنائي إلا من حيث محلها كما سبق أن أشرنا.

٣- الفساد المالي (الرشوة) وما يلحق بها:

جريمة الفساد المالي (الرشوة) وما يلحق بها تتمثل في استغلال الاشغال والمقاولات والتعهدات العامة للحصول على منافع غير مشروعة. وتختلف هذه الجريمة عن جريمة الإضرار بقصد الجريمة، حيث يمكن تحقيق الجريمة حتى لو لم يحدث ضرر فعلي بالمصلحة المحمية، بل يكفي أن يكون هناك احتمالية وجود ضرر. وبالتالي، تعتبر جريمة الفساد المالي من جرائم الخطر وليس الضرر، حيث يكفي لتحقيقها مجرد سعي المرتكب للحصول على منفعة من المصلحة التي يجب عليه حمايتها. وفي المقابل، تتطلب جريمة الإضرار بقصد الجريمة وجود ضرر فعلي في المصلحة المحمية. كما تختلف جريمة الفساد المالي عن الجريمة السابقة في أنه لا يُشترط فيها توافر القصد الخاص، بل يكفي وجود القصد الجنائي العام (العلم والإرادة).[١]

٤-الرشوة المعلوماتية والدخول الغير مشروع للأنظمة المعوماتية:

الرشوة المعلوماتية هي جريمة تأثرت بشكل كبير بتطور التكنولوجيا والتحول الرقمي. ولم تعد الرشوة تقتصر على المال المادي فحسب، بل يمكن أن تتم عن طريق تبادل المعلومات، البرامج، أو النظم المعلوماتية. حيث تعتبر هذه الجريمة انتهاكًا للأخلاقيات والمعايير القانونية وتهدف إلى تحقيق مكاسب غير قانونية للأفراد المعنيين.

ومع ذلك، فإن الرشوة المعلوماتية لا تخرج عن القواعد العامة لجريمة الرشوة في القانون الجنائي. فمع أنها تختلف في محلها، إلا أنها تشترك في طبيعة الجريمة وغرضها. ومع ذلك، يمكن أن يكون من الصعب إثبات الرشوة المعلوماتية بسبب طبيعتها الخفية والتقنيات المستخدمة في تنفيذها. حيث أن المنظومة الإدارية اللالكترونية أدت إلى ظهور جرائم

---

[١] – **نور الهموندي، جرائم الأموال العامة والوظيفة العامة في الشريعة الإسلامية والقانون، منشورات زين الحقوقية، ٢٠١٣، ص١٢٣.**

جديدة يمكن ارتكابها بواسطة الموظف العام، وتتميز هذه الجرائم بصعوبة إثباتها بسبب الدليل المعلوماتي والتكنولوجي الذي يتميز بالخفاء (١).

ونحن نرى، أن المنظومة الإدارية الالكترونية قد أدت إلى ظهور نوع جديد من جرائم الأموال العامة المحلقة حول المعلومات والتكنولوجيا. تشمل هذه الجرائم الاختلاس والاستيلاء المعلوماتي، جرائم الضرر بالأموال والمصالح العامة، والرشوة المعلوماتية. وعلى الرغم من تغير محل هذه الجرائم، إلا أنها لا تخرج عن القواعد العامة لجرائم الأموال العامة والرشوة في القانون الجنائي. ومع ذلك، يتطلب إثبات هذه الجرائم استخدام دليل معلوماتي وتقني يتميز بالخفاء، مما يزيد من تعقيدية إثباتها ومسؤولية التحقيق فيها.

ودولة الإمارات العربية المتحدة تعتبر من أكثر الدول التي اهتمت بمكافحة الجرائم الإلكترونية، ومنها جريمة الدخول غير المشروع إلى النظام المعلوماتي، حيث نصت المادة (٢) من قانون مكافحة الشائعات والجرائم الإلكترونية رقم (٣٤) لسنة ٢٠٢١ لدولة الإمارات العربية المتحدة على تجريم التوصل والوصول والدخول إلى موقع أو نظام معلوماتي بغير وجه حق والمعاقبة على ذلك وقد تضمنت هذه المادة ثلاث صور من التجريم[٢] :

١- **الصورة الأولى:** وهي التوصل بغير وجه حق إلى موقع أو نظام معلوماتي.

٢- **الصورة الثانية :** إذا ترتب على الفعل إلغاء أو حذف أو تدمير أو إفشاء أو تغيير أو إعادة نشر بيانات أو معلومات .

---

(١) – صفاء فتوح جمعة، الإطار القانوني والفني للتحول الرقمي في المنظمات الحكومية، مرجع سابق، ص٦٢٠.

(٢) – تنص المادة (٢) من قانون مكافحة الشائعات والجرائم الالكترونية رقم (٣٤) لسنة ٢٠٢١ لدولة الإمارات العربية المتحدة"

١. يعاقب بالحبس والغرامة التي لا تقل عن (١٠٠،٠٠٠) مائة ألف درهم ولا تزيد على (٣٠٠،٠٠٠) ثلاثمائة ألف درهم، أو بإحدى هاتين العقوبتين، كل من اخترق موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات.

٢. وتكون العقوبة الحبس مدة لا تقل عن (٦) ستة أشهر والغرامة التي لا تقل عن (١٥٠،٠٠٠) مائة وخمسون ألف درهم ولا تزيد على (٥٠٠،٠٠٠) خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين، إذا ترتب على الاختراق إحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أو الحصول على أي بيانات أو معلومات أو خسارة سريتها.

٣. وتكون العقوبة الحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن (٢٠٠،٠٠٠) مائتي ألف درهم ولا تزيد على (٥٠٠،٠٠٠) خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين، إذا كان الاختراق بغرض الحصول على البيانات أو المعلومات لتحقيق غرض غير مشروع".

- الصورة الثالثة : إذا كانت البيانات أو المعلومات ذات طابع شخصي.

وأكد المشرع الإتحادى الإماراتى فى المادة الثالثة من قانون مكافحة الشائعات والجرائم الإلكترونية رقم (٣٤) لسنة ٢٠٢١ على عقوبة اختراق الأنظمة المعلوماتية الخاصة بمؤسسات الدولة[١].

كما نصت المادة الرابعة من القانون على عقوبة من تسبب عمداً في الإضرار أو تدمير أو إيقاف أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات [٢].

كما نصت المادة الخامسة من القانون على عقوبة الإضرار بالأنظمة المعلوماتية لإحدى مؤسسات الدولة والمرافق الحيوية [٣] .

كما نصت المادة السادسة على عقوبة الاعتداء على البيانات والمعلومات الشخصية[٤].

---

(١) - المادة (٣) من قانون مكافحة الشائعات والجرائم الالكترونية رقم (٣٤) لسنة ٢٠٢١ لدولة الإمارات العربية المتحدة. حيث نصت على أنه" ١- يعاقب بالسجن المؤقت والغرامة التي لا تقل عن (٢٠٠,٠٠٠) مائتي ألف درهم ولا تزيد على (٥٠٠,٠٠٠) خمسمائة ألف درهم، كل من اخترق موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات عائدة لمؤسسات الدولة. ٢-وتكون العقوبة السجن مدة لا تقل عن (٥) خمس سنوات والغرامة التي لا تقل عن (٢٥٠,٠٠٠) مائتين وخمسين ألف درهم ولا تزيد على (١,٥٠٠,٠٠٠) مليون وخمسمائة ألف درهم، إذا ترتب على الاختراق إحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات أو خسارة سريتها أو وقعت الجريمة نتيجة لهجمة إلكترونية.٣- وتكون العقوبة السجن مدة لا تقل عن (٧) سنوات والغرامة التي لا تقل عن (٢٥٠,٠٠٠) مائتين وخمسين ألف درهم ولا تزيد على (١,٥٠٠,٠٠٠) مليون وخمسمائة ألف درهم، إذا كان الاختراق بغرض الحصول على البيانات أو المعلومات الخاصة بتلك الجهات المنصوص عليها بالفقرة الأولى من هذه المادة".

(٢) - المادة (٤) من قانون مكافحة الشائعات والجرائم الالكترونية رقم (٣٤) لسنة ٢٠٢١ لدولة الإمارات العربية المتحدة. حيث نصت على أنه " ١- يعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن (٥٠٠,٠٠٠) خمسمائة ألف درهم ولا تزيد على (٣,٠٠٠,٠٠٠) ثلاثة ملايين درهم، أو بإحدى هاتين العقوبتين، كل من تسبب عمداً في الإضرار أو تدمير أو إيقاف أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات.٢- تكون العقوبة السجن المؤقت والغرامة التي لا تقل عن (٥٠٠,٠٠٠) خمسمائة ألف درهم ولا تزيد على (٣,٠٠٠,٠٠٠) ثلاثة ملايين درهم، إذا كان الإضرار قد لحق جهة مصرفية أو إعلامية أو صحية أو علمية، أو إذا كان الغرض من ذلك تحقيق أمر غير مشروع أو وقعت الجريمة نتيجة لهجمة الكترونية".

(٣) - المادة (٥) من قانون مكافحة الشائعات والجرائم الالكترونية رقم (٣٤) لسنة ٢٠٢١ لدولة الإمارات العربية المتحدة. حيث نصت المادة على أنه "يعاقب بالسجن المؤقت والغرامة التي لا تقل عن (٥٠٠,٠٠٠) خمسمائة ألف درهم ولا تزيد على (٣,٠٠٠,٠٠٠) ثلاثة ملايين درهم، كل من تسبب عمداً في الإضرار أو تدمير أو إيقاف أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، عائدة لمؤسسات الدولة أو أحد المرافق الحيوية. فإذا وقعت الجريمة نتيجة لهجمة إلكترونية أعتبر ذلك ظرفاً مشدداً.

(٤) - المادة (٦) من قانون مكافحة الشائعات والجرائم الالكترونية رقم (٣٤) لسنة ٢٠٢١ لدولة الإمارات العربية المتحدة. حيث نصت على أنه " ١-يعاقب بالحبس مدة لا تقل عن (٦) ستة أشهر والغرامة التي لا تقل عن (٢٠,٠٠٠) عشرين ألف درهم ولا تزيد على (١٠٠,٠٠٠) مائة ألف درهم، أو بإحدى هاتين العقوبتين، كل من حصل أو استحوذ أو عدل أو أتلف أو أفشى أو سرب أو ألغى أو حذف أو نسخ أو نشر أو أعاد نشر بغير تصريح بيانات أو معلومات شخصية

كما نصت المادة السابعة من المرسوم على عقوبة الاعتداء على البيانات والمعلومات الحكومية [1].

أما التشريع الكويتي، فقد حددت المادة (٢) من القانون رقم (٦٣) لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات عقوبات الدخول غير المشروع إلى أنظمة الحاسوب ومعالجة البيانات والشبكات المعلوماتية ".[2]

ونحن نرى، كون المادة (٢) من القانون الكويتي رقم (٦٣) لسنة ٢٠١٥ تحدد عقوبات جرائم الدخول غير المشروع إلى أنظمة الحاسوب ومعالجة البيانات والشبكات المعلوماتية. فتعتبر هذه المادة إجراء قانوني هام لمكافحة جرائم تقنية المعلومات وحماية الأنظمة

إلكترونية، باستخدام تقنية المعلومات أو وسيلة تقنية معلومات. ٢- فإذا كانت البيانات أو المعلومات المشار إليها في البند (١) من هذه المادة، تتعلق بفحوصات أو تشخيص أو علاج أو رعاية أو سجلات طبية أو حسابات مصرفية أو بيانات ومعلومات وسائل الدفع الإلكترونية عد ذلك ظرفاً مشدداً. ٣- ويعاقب بالحبس والغرامة، أو بإحدى هاتين العقوبتين، كل من تلقى أي من البيانات والمعلومات المشار إليها بالبندين (١)، (٢) من هذه المادة، واحتفظ بها أو خزنها أو قبل التعامل بها أو استخدامها رغم علمه بعدم مشروعية الحصول عليها".

(١) - المادة (٧) من قانون مكافحة الشائعات والجرائم الالكترونية رقم (٣٤) لسنة ٢٠٢١ لدولة الإمارات العربية المتحدة. حيث نصت على أنه " ١-يعاقب بالسجن المؤقت مدة لا تقل عن (٧) سبع سنوات والغرامة التي لا تقل عن (٥٠٠,٠٠٠) خمسمائة ألف درهم ولا تزيد على (٣,٠٠٠,٠٠٠) ثلاثة ملايين درهم كل من حصل أو استحوذ أو عدل أو أتلف أو أفشى أو سرب أو ألغى أو حذف أو نسخ أو نشر أو أعاد نشر بغير تصريح بيانات أو معلومات حكومية سرية. ٢- وتكون العقوبة السجن المؤقت مدة لا تقل عن (١٠) سنوات والغرامة التي لا تقل عن (٥٠٠,٠٠٠) خمسمائة ألف درهم ولا تزيد على (٥,٠٠٠,٠٠٠) خمسة ملايين درهم إذا ترتب على الأفعال المنصوص عليها بالبند (١) من هذه المادة أضراراً للدولة، أو إذا ترتب عليها فقدان سرية عمل الأنظمة والبرمجيات الإلكترونية الخاصة بالمنشآت العسكرية والأمنية وما يتعلق بالاتصال ونقل المعلومات السرية.٣-ويعاقب بالسجن المؤقت كل من تلقى أي من البيانات والمعلومات المشار إليها بالبند (١) من هذه المادة، واحتفظ بها أو خزنها أو قبل التعامل بها أو استخدامها رغم علمه بعدم مشروعية الحصول عليها".

(2) – المادة (2) من القانون رقم (63) لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات الكويتي. "*يعاقب بالحبس مدة ال تجاوز ستة أشهر وبغرامة ال تقل عن خمسمائة دينار وال تجاوز ألفي دينار أو بإحدى هاتين العقوبتين، كل من أرتكب دخولاً غير مشروع إلى جهاز حاسب آلي أو إلى نظامه أو إلى نظام معالجة إلكترونية للبيانات أو إلى نظام إلكتروني مؤتمت أو إلى شبكة معلوماتية.*

فإذا ترتب على هذا الدخول إلغاء أو حذف أو إتلاف أو تدمير أو إفشاء أو تغيير أو إعادة نشر بيانات أو معلومات، فتكون العقوبة الحبس مدة لا تجاوز سنتين والغرامة التي لا تقل عن ألفي دينار وال تجاوز خمسة آالف دينار أو بإحدى هاتين العقوبتين.

فإذا كانت تلك البيانات أو المعلومات شخصية فتكون العقوبة الحبس مدة ال تجاوز ثالث سنوات والغرامة التي لا تقل عن ثلاثة آالف دينار ولا تجاوز عشرة آالف دينار أو بإحدى هاتين العقوبتين ويعاقب بالحبس مدة لا تجاوز خمس سنوات وبغرامة لا تقل عن ثلاثة آالف دينار ولا تجاوز عشرين ألف دينار أو بإحدى هاتين العقوبتين، كل من ارتكب أياً من الجرائم المنصوص عليها أعلاه أو سهل ذلك للغير وكان ذلك أثناء أو بسبب تأدية وظيفته.

الإلكترونية. ووفقًا للمادة، يعاقب المرتكب على دخول غير مشروع إلى جهاز حاسوب أو نظامه أو نظام معالجة إلكترونية للبيانات أو نظام معلوماتي بالحبس والغرامة. إذا ترتب على هذا الدخول إلغاء أو حذف أو إتلاف أو تدمير أو إفشاء أو تغيير أو إعادة نشر البيانات أو المعلومات، فإن العقوبة تكون الحبس والغرامة. وإذا كانت البيانات أو المعلومات التي تمت معاقبة الدخول غير المشروع إليها شخصية، فإن العقوبة تزيد لتصل إلى الحبس والغرامة الأعلى. كما يتم معاقبة أي شخص يسهل للآخرين ارتكاب هذه الجرائم أثناء أداء وظيفته.

وتهدف هذه المادة إلى تأمين الأنظمة الإلكترونية وحماية البيانات والمعلومات من الاختراق غير المشروع. وتعكس التشريعات القانونية الحاجة الملحة لتعزيز الأمن الإلكتروني وتوفير بيئة آمنة للتعامل الإلكتروني في المؤسسات العامة والخاصة.

كما أشارت المادة (٣) من القانون رقم (٦٣) لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات على عقوبة ارتكاب الدخول غير المشروع إلى موقع أو نظام معلوماتي بقصد الحصول على بيانات أو معلومات حكومية سرية بموجب القانون [١].

ونحن نرى، أيضاً كون المادة (٣) من القانون الكويتي رقم (٦٣) لسنة ٢٠١٥ حددت عقوبة ارتكاب الدخول غير المشروع إلى موقع أو نظام معلوماتي بقصد الحصول على بيانات أو معلومات حكومية سرية بموجب القانون، وإذا ترتب على هذا الدخول إلغاء أو إتلاف أو تدمير أو نشر أو تعديل تلك البيانات أو المعلومات، فإن العقوبة تصبح الحبس والغرامة الأعلى. كما تهدف المادة إلى حماية البيانات والمعلومات الحكومية السرية من الوصول غير المشروع، وتجريم أي محاولة للحصول على هذه البيانات بطرق غير قانونية. وتشير المادة أيضًا إلى أهمية حماية حسابات عملاء المنشآت المصرفية وعدم السماح بالوصول غير المشروع إلى معلوماتهم المصرفية الحساسة. ويمكن ربط هذه المادة بالجرائم الجنائية في

---

(١) – المادة (3) من القانون رقم (63) لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات الكويتي. "يعاقب بالحبس مدة لا تجاوز ثالث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين كل من: ١- ارتكب دخولاً غير مشروع إلى موقع أو نظام معلوماتي مباشرة أو عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية بحكم القانون . فإذا ترتب على ذلك الدخول إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو نشرها أو تعديلها، وتكون العقوبة الحبس مدة ال تجاوز عشر سنوات والغرامة التي ال تقل عن خمسة آلاف دينار ولا تجاوز عشرين ألف دينار أو بإحدى هاتين العقوبتين . ويسري هذا الحكم على البيانات والمعلومات المتعلقة بحسابات عملاء المنشآت المصرفية".

المنظومة الإدارية الإلكترونية للموظف العام، بإن الموظف العام الذي يرتكب جريمة دخول غير مشروع إلى الأنظمة الإلكترونية أو المواقع أو النظم المعلوماتية بقصد الحصول على بيانات أو معلومات سرية قد يتعرض لعقوبات الحبس والغرامة وفقًا للمادة المذكورة. وتعكس هذه المادة أهمية حماية البيانات والمعلومات الحكومية وضرورة توفير أنظمة أمنية قوية للتصدي للتهديدات الإلكترونية والتسلل غير المشروع. وتعزز القانونية والمسؤولية القانونية للموظف العام في التعامل مع الأنظمة الإلكترونية وضمان سلامتها وسرية المعلومات المخزنة فيها.

أما المُشرع المصرى فقد أشار فى المادة (١٤) من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات إلى عقوبة كل من دخل عمدا أو دخل بخطأ غير عمدى وبقى بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتى محظور الدخول عليه. [١]

كما أشارت المادة (١٥) من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات المصري إلى عقوبة كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتى مستخدما حقا مخولا له، فتعدى حدود.[٢]

كما أشارت المادة (١٧) من ذات القانون إلى عقوبة على كل من أتلف أو عطل أو عدل مسار أو ألغي كلياً أو جزئياً متعمداً وبدون وجه حق، البرامج والبيانات أو المعلومات المخزنة أو المعالجة أو المولدة أو المخلقة علي أي نظام معلوماتي ومافي حكمه[١]."

---

(١) – المادة (١٤) من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات المصري. "يعاقب بالحبس مدة لا تقل عن سنة ، وبغرامة لا تقل عن خمسين ألفا جنيه ولا تجاوز مائة ألف جنيه،أو بإحدى هاتين العقوبتين ، كل من دخل عمدا أو دخل بخطأ غير عمدى وبقى بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتى محظور الدخول عليه. فإذا نتج عن ذلك الدخول إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة علي ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي ، تكون العقوبة الحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتى ألف جنيه ،أو بإحدي هاتين العقوبتين."

(٢) – المادة (١٥) من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات المصري. "يعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتى مستخدما حقا مخولا له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول".

كما نصت المادة (١٨) على عقوبة كل من أتلف أو عطل أو أبطأ أو اخترق بريدا إلكترونيا أو موقعا أو حسابا خاصا بأحد الناس[٢].

كما نصت المادة (٢٠)على عقوبة كل من دخل عمداً، أو دخل بخطأ غير عمدى وبقى بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعا او بريدا إلكترونيا أو حسابا خاصا أو نظاما معلوماتيا يدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكا لها، أو يخصها[٣]."

وأخيراً نصت المادة (٢١) على عقوبة كل من تسبب متعمدا في إيقاف شبكة معلوماتية عن العمل أو تعطيلها أو الحد من كفاءة عملها أو التشويش عليها أو إعاقتها أو اعتراض عملها أو أجرى بدون وجه حق معالجة الكترونية للبيانات الخاصة بها [٤]

---

(١) – المادة (١٧) من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات المصري. " يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه ، أو بإحدي هاتين العقوبتين، كل من أتلف أو عطل أو عدل مسار أو ألغي كلياً أو جزئياً متعمداً وبدون وجه حق، البرامج والبيانات أو المعلومات المخزنة أو المعالجة أو المولدة أو المخلقة علي أي نظام معلوماتي ومافي حكمه ، أيا كانت الوسيلة التي استخدمت في الجريمة.

(٢) – المادة (١٨) من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات المصري. "يعاقب بالحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من أتلف أو عطل أو أبطأ أو اخترق بريدا إلكترونيا أو موقعا أو حسابا خاصا بأحد الناس. فإذا وقعت الجريمة على بريد إلكترونى أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة ، تكون العقوبة الحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتى ألف جنيه، أو بإحدى هاتين العقوبتين,

(٣) – المادة (٢٠) من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات المصري. "يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتى ألف جنيه، أو بإحدي هاتين العقوبتين ، كل من دخل عمداً، أو دخل بخطأ غير عمدى وبقى بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعا او بريدا إلكترونيا أو حسابا خاصا أو نظاما معلوماتيا يدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكا لها، أو يخصها. فإذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية، تكون العقوبة السجن، والغرامة التى لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه. وفى جميع الأحوال، إذا ترتب على أى من الأفعال السابقة إتلاف تلك البيانات أو المعلومات أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتى أو البريد الإلكترونى، أو تدميرها أو تشويهها أو تغييرها أو تغيير تصاميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها ، أو إلغاؤها كليا أو جزئيا، بأى وسيلة كانت، تكون العقوبة السجن، والغرامة التى لا تقل عن مليون جنيه ولا تجاوز خمسة ملايين جنيه.

(٤) – المادة (٢١) من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات المصري. "يعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لاتقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى

الخاتمة

صدرت قوانين مكافحة الجرائم الإلكترونية في الكويت ومصر ودولة الإمارات العربية المتحدة، وتحديداً القانون رقم ٦٣ لسنة ٢٠١٥ في الكويت والقانون رقم ١٧٥ لسنة ٢٠١٨ في مصر، والقانون رقم (٣٤) لسنة ٢٠٢١ لدولة الإمارات، ويتضمن القوانين العديد من أنواع الجرائم التي يمكن للموظف العام ارتكابها في سياق التكنولوجيا والمعلومات، مثل جريمة الدخول غير المشروع إلى مواقع أو أنظمة معلوماتية، وجريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية. وبموجب هذه القوانين، يتم تنظيم وتجريم هذه الأعمال غير القانونية، وتُفرض عقوبات على المتسببين فيها، بما في ذلك العقوبات القانونية والغرامات المالية. وتهدف تلك القوانين إلى حماية سلامة البيانات والمعلومات وضمان سير العمليات التكنولوجية بطريقة آمنة وموثوقة. كما إن وجود هذه القوانين يساعد في توعية الموظفين العامين بأهمية الالتزام بالقوانين والقيم الأخلاقية في استخدام التكنولوجيا والمعلومات، ويُشدد على ضرورة النزاهة والثقة في أداء وظائفهم العامة. وبالتالي، يُعزز هذا الإطار القانوني العمل الحكومي المنظم والمسؤول فيما يتعلق بتقنية المعلومات ويحمي المصالح العامة. ومن خلال هذا البحث قد توصلنا إلى عدد من النتائج، والتوصيات، سوف نوضحها على النحو التالي:

أولاً- النتائج:

هاتين العقوبتين ، كل من تسبب متعمدا في إيقاف شبكة معلوماتية عن العمل أو تعطيلها أو الحد من كفاءة عملها أو التشويش عليها أو إعاقتها أو اعتراض عملها أو أجرى بدون وجه حق معالجة الكترونية للبيانات الخاصة بها. ويعاقب كل من تسبب بخطئه في ذلك بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لاتقل عن خمسين ألف جنيه ولا تجاوز مائتى الف جنيه، أو بإحدى هاتين العقوبتين. فإذا وقعت الجريمة على شبكة معلوماتية تخص الدولة أو أحد الأشخاص الاعتبارية العامة او تمتلكها او تدار بمعرفتها تكون العقوبة السجن المشدد، وبغرامة لاتقل عن خمسمائة ألف جنيه ولاتجاوز مليون جنيه.

١- المشرع المصري أحسن في النص على الحكم بعزل الموظف العام في حال ارتكابه جريمة أثناء وبسبب وظيفته، مما يعزز الثقة والنزاهة المفترضة في شغل المناصب العامة.

٢- لم يتطرق المشرع الكويتي في القانون الكويتي رقم (٦٣) لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات الى توضيح المقصود بالمعلومات الحكومية وسرية المعلومات وتحديدها مثل ما نص عليه المشرع المصري والإماراتي.

٣- عدم وجود نص خاص بتجريم إحجام الشخص الاعتباري عن ابلاغ الجهات الرسمية في حال وقوعه ضحية الجريمة الإلكترونية في القانون المصري والإماراتي والكويتي.

٤- ربط المشرع الكويتي مفهوم الاحتيال الإلكتروني بقصد الحصول على منفعة دون وجه حق أو الإضرار بالغير، وكان من المستحسن عدم ربط الاحتيال الإلكتروني بوجود قصد خاص كالحصول على المنفعة أو الإضرار بالغير ، إذ من المعلوم أن كثير من عمليات الاحتيال الإلكتروني يتم ارتكابها من أجل المتعة الذاتية ، ومحاولة لفت الأنظار، وإثبات الذات والتحدي.

٥- أغفل المشرع الكويتي تعريف (التداخل) وهو فعلٌ يختلف عن الدخول غير المشروع ، ويختلف أيضا عن االلتقاط ، وهو يتعلق بمحاولة المجرم (الجاني) اعتراض الموجات والإشارات بقصد الاطلاع على محتواها ، او بقصد التشويش ، وهو ما يحدث غالبا في البث التلفزيوني المشفر.

٦- أغفل المشرع الكويتي النص على تجريم فعل (البقاء) الذي يتحقق في حالة ما اذا كان الجاني مسموحا له بالولوج لفترة زمنية محددة ، ولكنه يتعمد البقاء بعد انقضاء تلك الفترة، وهو يجعل من بقاؤه بقاء غير مشروع، وهو ما نصت عليه الاتفاقية العربية لمكافحة الجريمة المعلوماتية، والتي صادقت عليها الكويت بموجب القانون رقم ٦٠ لسنة ٢٠١٣.

٧- اشترط المشرع الكويتي لقيام جريمة الاحتيال االلكترونية أن يكون من شان الطرق والوسائل المستخدمة في الاحتيال من شأنها خداع المجني عليه ، وقد جانب المشرع الكويتي التوفيق في هذه المسألة ؛ إذ من الصعب تقبل هذا الشرط في جريمة الاحتيال االلكتروني لكون العالم االلكتروني في حقيقته هو عالم معقد يعتمد على المعرفة الجيدة بوسائل تقنية المعلومات وهو ما يجعله غالبية مستخدمي الفضاء االلكتروني ، ومن ثم فقد كان من الافضل عدم ربط قيام جريمة الاحتيال االلكتروني بهذا الشرط المنصوص عليه بالفقرة الخامسة من المادة الثالثة من القانون.

ثانياً- التوصيات:

في ضوء هذه الإطلالة السريعة على الإطار القانوني للجرائم الجنائية في المنظومة الإدارية الإلكترونية للموظف العام في ضوء التشريع المصري والكويتي والإماراتي، فإننا نوصي بالآتي:

١- نوصى المشرع الكويتي تبني التجريم بواقعية ووضوع لا لبس ولا غموض فيهما بتفادي أنماط وصور مطاطة من أنواع السلوك في مجال الجرائم الإلكترونية في القانون الكويتي رقم (٦٣) لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات حتى لا تتناقض أسس الحماية الموضوعية أو تتعارض مع بعضها البعض، مع مراعاة المنظور المستقبلي ليتواكب مع التطور السريع في أشكال وأنماط وأدوات الجريمة الإلكترونية (المعلوماتية).

٢- نوصى المشرع الكويتي بإضافة نصوص قانونية في التشريع الكويتي تنظم الإجراءات الإلكترونية والإثبات الإلكتروني، وذلك لتعزيز الأمان والثقة في المعاملات الإلكترونية وضمان حماية البيانات والمعلومات، على غرار القانون المصري والإماراتي.

٣- نوصى المشرع الكويتي بتوضيح المقصود بالمعلومات الحكومية وسرية المعلومات وتحديدها بدقة في القانون الكويتي رقم (٦٣) لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات، لضمان وضوح القواعد القانونية والحماية اللازمة لهذه البيانات والمعلومات على غرار القانون المصري والإماراتي.

٤- نوصى المشرع الكويتى والإماراتى والمصرى بضرورة تدريب وتأهيل القضاة وجهات التحقيق والنيابة العامة على التعامل المتخصص مع الجرائم الإلكترونية والمعلوماتية، وفي هذا السياق يمكن إنشاء محاكم متخصصة في الجرائم الإلكترونية في مصر والإمارات والكويت.

٥- نوصى المشرع إضافة نص قانوني يجرم إحجام الشخص الاعتباري عن الإبلاغ الرسمي عند تعرضه لجريمة إلكترونية في القانون الكويتي والمصري والإماراتي، لحماية المصالح والحقوق والسلامة الشخصية للأفراد والمؤسسات.

٦- نوصى المشرع الكويتي والإماراتي والمصري بربط مفهوم الاحتيال الإلكتروني بالقصد العام للحصول على منفعة غير مشروعة أو إلحاق الضرر بالآخرين ، بغض النظر عن الدوافع الخاصة بالجاني، حيث يمكن أن يتم ارتكاب جرائم الاحتيال الإلكتروني لأسباب أخرى غير المنفعة الشخصية أو الضرر المقصود.

٧- نوصى المشرع الكويتي بتضمين تعريف لمفهوم التداخل في القانون الكويتي رقم (٦٣) لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات المتعلقة بالجرائم الإلكترونية، للتصدي لمحاولات اعتراض المجرمين على الموجات والإشارات بقصد التجسس أو التشويش، خاصة في البث التلفزيوني المشفر.

٨- نوصى المشرع الكويتي بإدراج تجريم فعل البقاء غير المشروع بعد انقضاء الفترة المسموح بها للوصول إلى نظام معلوماتي، وذلك لحماية الأنظمة والبيانات من الوصول غير المشروع واستغلالها.

قائمة المراجع

أولاً- المراجع العربية:

١- **ابن منظور**، أبو الفضل جمال الدين محمد بن مكرم، لسان العرب، دار صادر، بيروت، ٢٠١٠.

٢- **إبراهيم خليفة**، الجريمة والعقاب، أكاديمة نابف العربية للعلوم الأمنية، الرياض، ٢٠٠٨.

٣- **أحمد خليفة الملط**، الجرائم المعلوماتية، دار الفكر الجامعي، القاهرة، ٢٠٠٦.

٤- **جاسم محمد جندل**، الجرائم اللاكترونية، المعتز للنشر والتوزيع، عمان، ٢٠٢٢.

٥- **ذياب البداينة**، الجرائم المستحدثة والبحث العلمي في المجتمع العربي، بحث مقدم للندوة العلمية حول دور البحث العلمي في معالجة مشكلة الجريمة والإنحراف في الدول العربية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ٢٠١٠.

٦- **رفيق محمد سلام**، الحماية الجنائية للمال العام، دار النهضة العربية، القاهرة، ٢٠١٨.

٧- **سيد علي السيد محمد**، الجرائم الالكترونية، دار التعليم الجامعي، القاهرة، ٢٠٢٠.

٨- **سهير عبد المنعم**، الحماية الجنائية لنزاهة الوظيفة العامة، دار النهضة العربية، القاهرة، ٢٠١٦.

٩- **سامي علي حامد عياد**، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الإسكندرية، ٢٠١٥.

١٠- **صفاءة فتوح جمعة**، الإطار القانوني والفني للتحول الرقمي في المنظمات الحكومية، دار الفكر والقانون، المنصورة، مصر، ٢٠٢٢.

١١- **صفاء فتوح جمعة**، مسئولية الموظف العام في إطار تطبيق نظام الادارة الالكترونية، دار الفكر والقانون، المنصورة، جمهورية مصر العربية، ٢٠١٤.

١٢- **عبير شفيق الرحباني**، الجرائم الالكترونية ومخاطرها، دار الثقافة للنشر والتوزيع، عمان، ٢٠٢٠.

١٣- **عبد الفتاح بيومي حجازي**، جريمة غسل الأموال بين الوسائط الإلكترونية ونصوص التشريع، دار الفكر الجامعي، الإسكندرية، ٢٠٠٥.

١٤- **عبد الفتاح بيومي حجازي**، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دار الكتب القانونية، القاهرة، ٢٠٠٧.

١٥- **محمود أحمد محمد القرعان**، الجرائم الالكترونية، دار وائل للبطاعة والنشر، عمان، ٢٠١٧.

١٦- **محمد عبد الله إبراهيم**، المواجهة الأمنية لجرائم شبكة المعلومات الدولية، أكاديمية الشرطة المصرية، وزارة الداخلية، ٢٠١٦.

١٧- **محمد عبيد الكعبي**، الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٧.

١٨- **محمد عبد الله أبو بكر**، موسوعة جرائم المعلوماتية، جرائم الكمبيوتر والإنترنت، منشأة المعارف، الإسكندرية، ٢٠٠٦.

١٩- **محمد عبد الفتاح الأمير**، الوسيط في جرائم العدوان على المال العام، المجموعة العلمية للطبع والنشر، القاهرة، ٢٠٢١.

٢٠- **محمد أنور حماد**، الحماية الجنائية للأموال العامة، دار الفكر الجامعي، الإسكندرية، ٢٠٢٠.

٢١- **محمد علي سويلم**، السياسة الجنائية في مكافحة جرائم المال العام، المصرية للنشر والتوزيع، القاهرة، ٢٠١٩.

٢٢- **محمود أحمد سليمان البراشدي**، النظام القانوني لأموال المرافق في ظل سياسة الخصخصة، دار النهضة العربية، القاهرة، ٢٠١٧.

٢٣- **محمد محي الدين عوض**، القانون الجنائي، مبادئه الأساسية ونظرياته العامة، مطبعة جامعة القاهرة، القاهرة، ٢٠١٢.

٢٤- **محمد أبوزهرة**، الجريمة، دار الفكر العربي، القاهرة، ١٩٩٨.

٢٥- **نور الهموندي**، جرائم الأموال العامة والوظيفة العامة في الشريعة الإسلامية والقانون، منشورات زين الحقوقية، ٢٠١٣.

٢٦- **نسرين محمد نعمة الحسيني**، الجرائم اللالكترونية الواقعة على المال، المكتب الجامعي الحديث، القاهرة، ٢٠٢٠.

٢٧- **نهلا عبد القادر المومني**، الجرائم المعلوماتية، دار الثقافة، عمان، ٢٠٠٨.

٢٨- **وسيم حسام الدين الأحمد**، شرح قانون مكافحة الشائعات والجرائم اللالكترونية لدولة الإمارات العربية المتحدة، مرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١، دار الحافظ للنشر والتوزيع، الإمارات، ٢٠٢٣.

ثانياً- المراجع الأجنبية:

1- **John O'Reilly, Day Pitney LLP, Criminal Liability of Companies Survey , http://www.lexmundi.com/images/lexmundi/PDF/BusinessCrimes/CrimLiability USANew'/o20Jersey.pdf (last visited May 19, 2010).**

2- **Brożek, B., & Jakubiec, M. (2017). On the legal responsibility of autonomous machines. Artificial Intelligence and Law, 25(3), 293-304. https://doi.org/10.1007/s10506-017-9207-8.**

ثالثاً- التشريعات:

١. قانون رقم (٦٣) لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات الكويتي.

٢. مرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم اللالكترونية لدولة الإمارات العربية المتحدة.

٣. القانون رقم (١٧٥) لسنة ٢٠١٨ فى شأن مكافحة جرائم تقنية المعلومات.