بحث بعنوان

المواجهة الجنائية لجرائم تقنية المعلومات الماسة بأمن الدولة – دراسة مقارنة

الباحث

صابر رفاعي نظير أبو زيد

دارس الدكتوراه في القانون

كلية الحقوق

جامعة أسوان

ملخص الدراسة:

تناولت هذه الدراسة الجرائم التي تمس أمن الدولة بشقيه الداخلي والخارجي، والتي يتم ارتكابها استغلالا لوسائل تقنية المعلومات، حيث عمدت الى إيضاح هذه الصور من الجرائم، وتمييزها عن غيرها كما قدمت عرضا تحليليا يتضمن أركانها والجزاءات المنصوص عليها بشأنها، وذلك في كل من التشريعين المصري والإماراتي، وتوصلت الدراسة لعدد من النتائج، أهمها تسوية المشرع الإماراتي بين الشروع والفعل في التام في هذه الجرائم على عكس المشرع المصري الذي قرر عقوبة موحدة لهذه الجرائم كافة، كما اعتبر المشرع الإماراتي هذه الجرائم مستقلة، بينما اعتبر المشرع المصري أن مساس جرائم تقنية المعلومات بأمن الدولة ظرفا مشددا، وأوصت الدراسة بتعديل قانون مكافحة جرائم تقنية المعلومات واعتبار الجرائم المنصوص عليها بالمادة ٢٠ جرائم ماسة بأمن الدولة بصرف النظر عن القصد منها.

كلمات مفتاحية:

تقنية معلومات – أمن الدولة – الجرائم الإلكترونية.

Abstract:

This study addressed crimes that affect the state's security, both internal and external, and which are committed by exploiting information technology. It sought to clarify these types of crimes, distinguish them from others, and provided an analytical presentation that includes their elements and the penalties stipulated for them, in both Egyptian and Emirati legislation, The study reached a number of conclusions, the most important of which is that the UAE legislator equates the attempt and the completed act in these crimes, unlike the Egyptian legislator, who decided on a unified penalty for all these crimes. The UAE legislator also considered these crimes to be independent, while the Egyptian legislator considered the threat of information technology crimes to state security to be an aggravating circumstance, The study recommended amending the Anti-Cybercrime Law and considering the crimes stipulated in Article 20 as crimes that affect state security, regardless of their intent.

Key words:

Information Technology-state security-cybercrime.

المقدمة:

إذا كانت تقنية المعلومات تُعد أحد المظاهر الايجابية للعصر الراهن، فإن استخدام هذه التقنيات كان له جانبه السَّلبي والذي ألقى بظله على الأشخاص والدول، حيث انتشر إساءة استخدام هذه التقنيات، واستعمالها فيما يُخالف القوانين، وما يُعد اعتداء على حقوق المُجتمع بعديد من الصور، وإذا كان الوضع الغالب هو استخدام تقنية المعلومات في الاعتداء على حقوق الأشخاص، فإن الواقع يَشهد باستخدامها في النَّيل من الأمن القومي والخروج على مُقتضياته، إذ أصبح الاعتماد عليها في ارتكاب الجرائم الماسة بأمن الدولة هو مما شاع في ارتكاب هذا النوع من الجرائم، وذلك استنادا لسهولة استخدامها، وسرعة وقوة تأثيرها، الأمر الذي دفع الجناة لاستخدامها من جهة، ودفع المشرع لسنّ القوانين المُستحدثة لمواجهتها من جهة أخرى.

وتُمثل جرائم الاعتداء على أمن الدولة الداخلي والخارجي تَحدي كبير يواجه المشرع الوطني في مُختلف المُجتمعات الإنسانية، وذلك بسبب فداحة الأضرار التي قد تَنتُج عن مثل هذه الجرائم التي قد يَترتب عليها إنهيار مُجتمعات إنسانية بأكملها، وقد كانت الفترة الأخيرة فترة عسيرة بالنسبة لكثير من الدول العربية، حيث تَعرّض عديد منها لهذه الجرائم التي مازالت تُحاول أن تَتعافى منها، وتُعيد لمجتمعاتها التوازن الاجتماعي والسياسي والاقتصادي

وقد اختلفت السياسة التشريعية في مواجهة هذا النوع من الجرائم، حيث عَمدت بعض التشريعات إلى معالجتها في ضوء القواعد العامة في قانون العقوبات، بينما فضّل المُشرع في نُظُم أخرى أن يواجه الاعتداء على أمن الدولة باستخدام وسائل تقنية المعلومات عن طريق التشريعات المُتخصصة في مكافحة الجرائم الالكترونية، وهو ما انتهجه المشرع الاماراتي عبر المرسوم بقانون اتحادي رقم (٣٤) ، لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الالكترونية، والمشرع المصري عبر قانون مكافحة جرائم تقنية المعلومات رقم (١٧٥) ، لسنة ٢٠١٨، مع اختلاف المعالجة التشريعية، فبينما عَدّ المشرع الإماراتي استخدام تقنية المعلومات في ارتكاب الجرائم الماسة بأمن الدولة هو جريمة مستقلة بذاتها، عَدّ المشرع المصري هذا الاستخدام ظرف مُشدد يَستوجب تغليظ العقوبة المقررة.

أهمية البحث وسبب اختياره

تَستمد هذه الدراسة أهميتها من الاستخدام المُستحدث لوسائل تقنية المعلومات في ارتكاب الجرائم الماسة بأمن الدولة، والذي استوجب مُعالجة تشريعية خاصة تَتلائم مع طبيعة وخطورة هذه الجرائم من جهة، والذّاتية التي تَتسم بها جرائم تقنية المعلومات من جهة أخرى ، كما تأتي أهمية البحث فى مُحاولة للوصول إلى اليقين التشريعي لما سنّه المُشرع الإماراتي فيما يَتعلق بجرائم تقنية المعلومات الماسة بأمن الدولة وبيان مدى تأثره بالتشريعات الأخرى كالمشرع المصري ، كما يكمن سبب اختيار البحث حيث أنه يُعد من الأبحاث القليلة التى

تناولت جرائم تقنية المعلومات الماسة بأمن الدولة فى ضوء التشريع الإماراتي الحديث مقارنة بالتشريع المصري.

إشكالية البحث

تَتمثل إشكالية الدراسة في تنوع أنماط السلوك الاجرامي للجرائم الماسة بأمن الدولة والمُرتكبة بواسطة تقنية المعلومات، الأمر الذي يَخرج بها من حيز الحَصر، مما يُصعّب من مُهمة المُشرع في مكافحتها عن طريق نصوص التجريم المباشرة، وهو ما يَتبين في كل من القانونين الاماراتي والمصري، والَّذَين وضعا أحكاما عامة تُعد معها الجرائم الواردة في نصوصهما ماسة بأمن الدولة في حالات معينة، مما يَستوجب تطبيق قواعد استثنائية عليها وردت في قوانين أخرى. ونتج عن مشكلة الدراسة التساؤل الرئيس: **ما آليات المواجهة الجنائية لجرائم تقنية المعلومات الماسة بأمن الدولة في إطار قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨؟ وما الفروق التشريعية بينه وبين قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي رقم (٣٤) لسنة ٢٠٢١؟** ويتفرع عن هذا التساؤل عدد من الأسئلة الفرعية على النحو التالي:

١. ما ماهية جرائم تقنية المعلومات الماسة بأمن الدولة وأركانها؟
٢. ما الذي يميز جرائم تقنية المعلومات الماسة بأمن الدولة عن غيرها من الجرائم؟
٣. ما أركان جريمة تقنية المعلومات الماسة بأمن الدولة؟
٤. ما المواجهة الجزائية لجرائم تقنية المعلومات الماسة بأمن الدولة؟
٥. ما إجراءات جمع الاستدلالات والتحقيق فى جرائم تقنية المعلومات الماسة بأمن الدولة؟

أهداف البحث:

يَهدف البحث لتناول العديد من النقاط المُهمة على النحو الآتي:

١. بيان ماهية جرائم تقنية المعلومات الماسة بأمن الدولة وأركانها.
٢. التمييز بين جرائم تقنية المعلومات الماسة بأمن الدولة عن غيرها من الجرائم.
٣. توضيح أركان جريمة تقنية المعلومات الماسة بأمن الدولة.
٤. التعرف على المواجهة الجزائية لجرائم تقنية المعلومات الماسة بأمن الدولة.
٥. بيان إجراءات جمع الاستدلالات والتحقيق فى جرائم تقنية المعلومات الماسة بأمن الدولة.

منهج البحث:

اعتمدت الدراسة على المنهج الوصفي التحليلي من خلال توصيف الظاهرة المُتعلقة بالنصوص القانونية، مع القيام بتحليل نصوص التجريم والنصوص العقابية التي تناولت الجرائم محل البحث للوصول لأهم النتائج والتوصيات، كما استخدمت الدراسة المنهج المقارن بما ورد في التشريعين المصري والإماراتي، وبيان أهم الفروق التشريعية بين التشريعين ومدى تأثر أحدهما بالآخر.

خطة الدراسة

المبحث الأول: ماهية جرائم تقنية المعلومات الماسة بأمن الدولة وأركانها.

المبحث الثاني: المواجهة الجزائية لجرائم تقنية المعلومات الماسة بأمن الدولة.

المبحث الأول: ماهية جرائم تقنية المعلومات الماسة بأمن الدولة وأركانها

تمهيد وتقسيم:

إذا كانت وسائل تقنية المعلومات قد تدخلت في كافة جوانب الأنشطة الاجتماعية والاقتصادية وغيرها من مجالات الحياة، فإنها لم تكن بمعزل عن ارتكاب الجريمة، حيث تسببت هذه الوسائل في ظهور عدد كبير من الجرائم المستحدثة، والتي ارتبطت بها بصورة لصيقة، أما لوقوع الجريمة على وسائل تقنية المعلومات ذاتها، وإما لاعتماد الجريمة على هذه الوسائل كوسيلة لارتكابها، أو بمساهمتها في وقوع الجريمة، ولا يمكن القول باقتصار ارتباط وسائل تقنية المعلومات بنوع معين من الجرائم أو صور محددة للجرية، وإنما أصبحت الجرائم التي ترتكب باستخدامها عصية على الحصر الى الدرجة التي يمكن معها القول أن أغلب الجرائم في العصر الحالي يتصور ارتكابها بواسطة وسائل تقنية المعلومات بصورة أو بأخرى، حيث تدخلت هذه الوسائل في جرائم المصلحة العامة وجرائم الأشخاص والأموال، الى الدرجة التي دعت بعض الفقه للقول أن جرائم تقنية المعلومات هي صورة جديدة مستقلة للجريمة تختلف عن الجرائم التقليدية، ولا تعد مجرد وسيلة لارتكاب الجريمة، أو أداة يستخدمها الجاني لتسهيل ارتكاب جرائمه (محمد، ٢٠١٨، ١٧)[١].

المطلب الأول: مفهوم جرائم تقنية المعلومات الماسة بأمن الدولة.

المطلب الثاني: أركان جريمة تقنية المعلومات الماسة بأمن الدولة.

المطلب الأول: مفهوم جرائم تقنية المعلومات الماسة بأمن الدولة

يتضمن مفهوم جرائم تقنية المعلومات الماسة بأمن الدولة عنصرين رئيسين، الأول هو يتمثل في وسيلة ارتكاب الجريمة ويتبين من اعتماد الجاني عند ارتكابه لهذا النوع من الجرائم على واحدة أو أكثر من وسائل تقنية المعلومات، والثاني هو استهداف هذه الجرائم تهديد أمن الدولة بمفهومه القانوني، إذ بخلو الجريمة من أحد هذين العنصرين تفقد صفتها كجريمة تقنية معلومات ماسة بأمن الدولة، وهو ما يميز هذه الجريمة عن غيرها من جرائم تقنية المعلومات، والجرائم الماسة بأمن الدولة، فمناط التمييز في هذه الحالة هو اجتماع هذين الشرطين في الجريمة، بالإضافة الى ورودها ضمن جرائم أمن الدولة الواردة في المرسوم بقانون رقم ٣٤ لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الإلكترونية، أو قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨، وذلك طبقا لمبدأ شرعية الجرائم والعقوبات.

ويتميز تعريف جرائم تقنية المعلومات الماسة بأمن الدولة – كما سلف الذكر – باشتماله على عنصرين بحيث يؤدي غياب أحدهما الى انتفاء صفة هذه الجريمة فتتحول الى جريمة أخرى أو ينتفي عنها التجريم، وهو الأمر الذي يقتضي التصدي لتعريفها من هاتين الزاويتين، فمن زاوية جرائم تقنية المعلومات عرفها بعض الفقه بانها الجرائم التي تشمل صور السلوك الإجرامي المرتبط بشبكة الإنترنت أو أجهزة الحاسب الآلي (سويلم، ٢٠١٩، ١٤٤)[٢] كما عرفها فقه أخر بإنها الجرائم التي ترتكب بواسطة الشبكات أو الأنظمة الرقمية، أو داخل هذه الأنظمة (المري، ٢٠١٩، ٧٧)[٣] وأخيرا عرفها فقه ثالث بإنها الجرائم التي ترتكب بواسطة إحدى الوسائل الإلكترونية أو على احدى هذه الوسائل (الطوالبة، ٢٠١٨، ٩٠)[٤].

أما من زاوية التشريع فقد اغفل كلا من المشرعين الإماراتي والمصري التصدي لوضع تعريف محدد لجرائم تقنية المعلومات، حيث سلك المشرعان المسلك المعتاد للمشرع المعاصر، وهو ترك مهمة وضع التعريفات للفقه والقضاء، على اعتبار أن هذه المهمة تخرج عن اختصاص التشريع، وعليه فقد اقتصرت التعريفات الواردة في كلا من المرسوم بقانون رقم ٣٤ لسنة ٢٠٢١ والقانون رقم ١٧٥ لسنة ٢٠١٨ على تعريف تقنية المعلومات ذاتها باعتبارها وسيلة أو محل ارتكاب هذا النوع من الجرائم، فعرفها المشرع الاتحادي في المادة ١ من المرسوم بقانون رقم ٣٤ لسنة ٢٠٢١ بإنها "أي شكل من أشكال التقنيات المستخدمة في إنشاء وتخزين ومعالجة واستخدام وتبادل نظم المعلومات الإلكترونية، والمواقع الإلكترونية، والبرامج المعلوماتية، والشبكة المعلوماتية، أو أي من وسائل تقنية المعلومات"، وعرفها المشرع المصري في المادة ١ من القانون رقم ١٧٥ لسنة ٢٠١٨ بإنها "أي وسيلة أو مجموعة وسائل مترابطة أو غير مترابطة تستخدم لتخزين واسترجاع وترتيب وتنظيم ومعالجة وتطوير وتبادل المعلومات والبيانات ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة سلكيا أو لا سلكيا".

وأخيرا تصدى القضاء لتعريف تقنيات المعلومات، فعرفها القضاء الإماراتي في حكم محكمة تمييز دبي، الطعن رقم ٨٩٥ لسنة ٢٠١٥ جزائي، جلسة ٨ يونية ٢٠١٥ بإنها "أي وسيلة مرتبطة تتيح تخزين المعلومات الإلكترونية وإيصالها للآخرين، من خلال تخزين بيانات أو اِتصالات تقترن مع هذه الأداة، وهي وسائل لا يُمكن حصرها، فتشمل الحواسب الآلية والشبكة المعلوماتية، والهواتف الذكية، فالمناط أن تحتوي على نُظم معالجة وتخزين واِسترجاع وإرسال البيانات"، كما عرفها القضاء المصري في حكم محكمة النقض المصرية، الطعن رقم ١٥٨٠٢ لسنة ٩٠ قضائية، جلسة ٨ يونية ٢٠٢١ بإنها "وسائل تحقق خاصية تخزين واِسترجاع وتبادل المعلومات الإلكترونية"، أما الشق الثاني لجرائم تقنية المعلومات الماسة بأمن الدولة فيتمثل في الجرائم التي تهدد أمن الدولة، وهي الجرائم التي عرفها بعض الفقه على إنها الجرائم التي تهدد قدرة الدولة على حماية مصالحها من التهديدات الداخلية والخارجية، أو الجرائم التي تحد من جهود الدولة التي تهدف الدولة

من بذلها الى حماية حقها في البقاء، أو الجرائم التي تهدد وحدة الدولة واستقرارها السياسي (عويضة، ٢٠٢٠، ١١٤)[٥].

وعلى الرغم من وحدة غرض التشريعات الجنائية، واتفاقها على ضمان توفير الحماية الجنائية لأمن الدولة بصورة عامة، فإنها اختلفت في أسلوب تحقيق هذا الهدف، اذا اتجهت بعض التشريعات الى الفصل بين الأمن الداخلي والخارجي للدولة، بحيث يخص المشرع في هذه الحالة كل قسم منهما بأحكام خاصة (السويدي، ٢٠١٥، ٦١)[٦]، وهو النسق الذي اتبعه المشرع الاتحادي من خلال المرسوم بقانون اتحادي رقم ٣١ لسنة ٢٠٢١ بإصدار قانون الجرائم والعقوبات، وفي المقابل لم تفرق تشريعات أخرى بين المفهومين، إذ اعتبرت بعض مظاهر السلوك الإجرامي هي جرائم واقعة على أمن الدولة بصفة عامة دون أن تفرق بين الأمن الداخلي والخارجي، وهو مسلك المشرع الاتحادي من خلال المرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١.

وعلى هذا – وبالنظر للتعاريف السابقة – يمكن القول بأن جرائم تقنية المعلومات الماسة بأمن الدولة هي الجرائم التي ترتكب باستخدام الشبكات أو النظم المعلوماتية أو وسائل تقنية المعلومات والتي تهدد أمن الدولة سواء من جهة الداخل أو الخارج، وهي صورة إجرامية يلجأ من خلالها الجاني الى الوسائل الإلكترونية في سبيل تحقيق غايته التي تتمثل في النيل من مصالح الدولة العليا، سواء كانت هذه المصالح سياسية او اقتصادية او اجتماعية، وهي الجرائم الواردة بالمادة ٧١ من المرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الإلكترونية، والتي شملت النص على عشرين جريمة وردت بالمرسوم بالإضافة الى الحكم العام الوارد بالمادة والذي عد كافة الجرائم الواردة بمواد هذا القانون تقع ضمن نطاق الجرائم الماسة بأمن الدولة في حالة ارتكابها لمصلحة أو لحساب دولة أجنبية أو تنظيم أو جماعة إرهابية أو منظمة أو هيئة غير مشروعة.

ويلاحظ على مسلك المشرع الاتحادي من خلال المرسوم بقانون رقم ٣٤ لسنة ٢٠٢١ انه قسم جرائم أمن الدولة الى قسمين، حيث ضمّن القسم الأول جرائم تقنية المعلومات الماسة بأمن الدولة لذاتها، وهي جرائم تعد من جرائم أمن الدولة بغض النظر عن شخص مرتكبها او شخص المحرض على ارتكابها أو الدافع لارتكابها، إذ تصنف ضمن الجرائم الماسة بأمن الدولة في كل الأحوال، أما القسم الثاني من هذه الجرائم فقد نص عليه المشرع الاتحادي في عجز المادة ٧١ وتضمن كافة الجرائم التي نص عليها المرسوم بقانون رقم ٣٤ لسنة ٢٠٢١ في حالات معينة هي ارتكابها لصالح او حساب جهة مما نصت عليه المادة (منصوري، ٢٠٢١، ١١٤)[٧].

أما المشرع المصري فمن خلال المادة ٣٤ من قانون مكافحة الجرائم الإلكترونية رقم ١٧٥ لسنة ٢٠١٨، فحدد جرائم تقنية المعلومات عن طريق الهدف من ارتكابها، وذلك في حكم عام مفاده أن أي من الجرائم

المنصوص عليها بالقانون تعد من جرائم أمن الدولة اذا استهدفت تعريض سلامة المجتمع وأمنه للخطر، أو الإخلال بالنظام العام، أو الإضرار بالأمن القومي للدولة، أو مركزها الاقتصادي، أو تعطيل أحكام الدستور أو القوانين أو اللوائح، أو عرقلة أو منع السلطات العامة في الدولة عن ممارسة أعمالها، أو الإضرار بالسلام الاجتماعي أو الوحدة الوطنية (الغفلي، ٢٠٢١، ٣٩)[٨].

ويلاحظ على مسلك المشرع المصري انه لم يراع الذاتية التي تتصف بها الجرائم الماسة بأمن الدولة في القانون رقم ١٧٥ لسنة ٢٠١٨، – بعكس مسلكه في قانون العقوبات – إذ عد ارتكاب الجرائم الواردة في القانون رقم ١٧٥ استهدافا لأحد المقاصد الواردة بالمادة ٣٤ هو ظرف مشدد للجريمة يستوجب تشديد العقوبة، لا جريمة مستقلة بأحكامها، الأمر الذي يتعارض مع مسلك المشرع الإماراتي الذي يتضح من خلال المادة ٧١ من المرسوم بقانون رقم ٣٤ لسنة ٢٠٢١، إذ على الرغم من تضمن المادة ٢٠ لعدد من الجرائم التي تقع على الأنظمة المعلوماتية الخاصة بالدولة بما يعرض مصالح الدولة العليا للخطر إلا أن المشرع المصري أغفل الاعتراف لهذه الجرائم بمساسها بأمن الدولة إلا اذا ارتكبت لهدف مما نصت عليه المادة ٣٤ من القانون، وهو ما لا يتلاءم مع الحرص على حماية المصالح العليا للدولة من تعرضها للخطر.

وعلى هذا يمكن الذهاب الى أن المسلك التشريعي والصياغة التشريعية للمشرع الإماراتي كانا اكثر دقة وإحكاما مما جرى عليه المشرع المصري، وذلك من خلال التشريعين الإلكترونيين في الدولتين، فبينما حرص المشرع الاتحادي على تحديد جرائم تقنية المعلومات الماسة بأمن الدولة والنص عليها على سبيل التحديد بالإضافة الى تحديد حالات اعتبار أي جريمة مما ورد بالقانون هي من جرائم امن الدولة، اكتفى المشرع المصري بالهدف من الجريمة كمناط لاعتبارها من الجرائم الماسة بأمن الدولة، مما يترتب عليه استبعاد أي جريمة من النطاق المحدد طالما لم تستهدف أي من الأهداف الواردة بالمادة ٣٤ برغم تصور مساسها بأمن الدولة.

وتتسم جرائم تقنية المعلومات الماسة بأمن الدولة بعدد من السمات التي تميزها عن غيرها من الجرائم، وهي السمات التي ميزها بها المشرع في خروجه في التناول التشريعي عن القواعد العامة في التجريم والعقاب التي تخضع لها سائر الجرائم، وهو تمييز يفرضه لزوم المنطق القانوني، فمن ناحية يتسم المجرم في هذه الجرائم بعدد من الصفات أهمها قدرته على استخدام الوسائل الإلكترونية الحديثة بما يشمله ذلك من خبرة فنية ومهارة في التعامل مع هذه الوسائل، كما يتصف بخطورة إجرامية بالغة، إذ يعتقد أثناء ارتكابه للجريمة انه يؤدي واجب عقائدي أو سياسي أو اجتماعي وبالتالي لا يكترث لخطورة النتائج الإجرامية الناجمة عن جريمته، أو فداحة الخسائر التي يرتبها فعله (علي، ٢٠٢٠، ٨٠)[٩].

كما تتميز الجريمة ذاتها بقدرتها على اكتساب التعاطف من البعض، وذلك تبعا للظروف الخاصة بالجاني أو القضية التي يدعي تبنيها، الأمر الذي قد يصعب من مهمة ضبطها والقبض على مرتكبيها ومحاكمتهم،

بالإضافة للنتائج الإجرامية غير المعتادة التي قد تترتب عليها وتتمثل في الأضرار الفادحة التي قد تصيب الدولة والمجتمع جراء هذا النوع من الجرائم (نصار، ٢٠١٧، ٥٢)[١٠].

ويمكن التمثيل للتمييز التشريعي لهذا النوع من الجرائم فيما يلي:

أولا: الاستناد لعنصر الخطر في تجريم المساس بأمن الدولة عن طريق تقنية المعلومات: عد المشرع الاتحادي جرائم أمن الدولة التي ترتكب بواسطة تقنية المعلومات من جرائم الخطر، مما مؤداه عدم اشتراط تحقق النتيجة الإجرامية المترتبة على السلوك الإجرامي كمناط لتقرير العقاب، فتحقق النتيجة في حد ذاته لا يعد ضمن شروط قيام المسئولية الجنائية عن الفعل، فهو ليس من عناصر تحقق النموذج القانوني للجريمة، وهو ما يتبين من صياغة عدد من المواد الواردة في المرسوم بقانون رقم ٣٤ لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الإلكترونية، فعلى سبيل المثال تناولت المادة ٢٧ من المرسوم بقانون التحريض على عدم الانقياد للتشريعات، وهي الجريمة التي تقع تامة بمجرد التحريض حتى لو يلق هذا التحريض قبولا لدى الغير ولم يسفر عن أي نتائج مادية تتمثل في عدم الانقياد الفعلي، وهو ما ينطبق على الجرائم الواردة بالمواد ٢٠، ٢١، ٢٣، ٥٢، ٥٥ والتي تقع بمجرد ارتكاب الفعل دون توقف على تحقق النتيجة المرجوة منه (العاصمي، ٢٠٢٢، ١٠٥)[١١]، أما المشرع المصري فبرغم اتباعه لهذه القاعدة في قانون العقوبات المصري إلا انه خرج عنها في القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات، وهي النتيجة المنطقية على اعتباره مساس الجرائم الواردة بالقانون رقم ١٧٥ بأمن الدولة هو ظرف مشدد وليس جريمة مستقلة لها ذاتيتها، وبناء على ذلك تتبع جرائم تقنية المعلومات الماسة بأمن الدولة في التشريع المصري الجريمة الأصلية في سماتها، فتلحق في اعتبارها من جرائم الخطر أو الضرر الجريمة التي توفر لها التشديد بمساسها بأمن الدولة (سويلم، ٢٠١٩، ١١٨)[١٢].

ثانيا: الخروج على القواعد العامة في التدرج في العقاب: يلاحظ أن المشرع الإماراتي وإن كان قد التزم بقاعدة التدرج في العقاب في مواجهته الجنائية لأغلب الجرائم، إلا انه خرج على هذه القاعدة في جرائم تقنية المعلومات الماسة بأمن الدولة، حيث تسوي سياسته العقابية في العقاب بين الشروع والفعل التام في عدد من الحالات، وهو الوضع الذي يبرز من خلال عديد من النصوص القانونية مثل المواد ١٨١، ١٨٢ من المرسوم بقانون رقم ٣١ لسنة ٢٠٢١ بإصدار قانون الجرائم والعقوبات، والمادة ٩ من قانون مكافحة الجرائم الإرهابية رقم ٧ لسنة ٢٠١٤، وذلك في حالة ارتكاب الجرائم الواردة بها عن طريق احدى تقنيات المعلومات مما يعد مناطا لتطبيق المادة ٦٠ فقرة ٢ من المرسوم بقانون رقم ٣٤ لسنة ٢٠٢١، وهي الفقرة التي تشدد العقوبة في حالة ارتكاب أي جريمة لم ينص عليها قانون مكافحة الشائعات والجرائم الإلكترونية باستخدام وسيلة لتقنية المعلومات أو شبكة إلكترونية أو موقع إلكتروني (البلوشي، ٢٠٢٢، ١٢٢)[١٣]، بينما يقرر عقاب على الشروع في الجنح في حالات أخرى، الأمر الذي يتبين من خلال المادة ٥٧ من المرسوم بقانون رقم ٣٤

لسنة ٢٠٢١، والتي تضمنت حكما عاما مفاده العقاب على الشروع في كافة الجنح الواردة في المرسوم بقانون بنصف العقاب المفروض للجريمة التامة.

أما المشرع المصري فمن خلال المادة ٣٤ من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات فقد وحد العقوبات بطريقة استثنائية، حيث قرر عقوبة السجن المشدد لكافة الجرائم الواردة في القانون رقم ١٧٥ في حالة مساسها بأمن الدولة، فتسوي هذه المادة بين الجنح والجنايات من حيث العقاب في حالة ارتكابها على النحو الوارد في المادة ٣٤، بينما أتت المادة ٤٠ من القانون لتقرر نصف العقوبة على الشروع في الجنح الواردة في القانون (بطيخ، ٢٠٢٠، ٨٠)[١٤]، على غرار المادة ٥٧ من المرسوم بقانون رقم ٣٤ لسنة ٢٠٢١.

مما سبق يتبين أن المشرع المصري قد تمادى في الخروج على القواعد العامة في التدرج العقابي بصورة كبيرة قد لا تتلاءم مع الخطورة الإجرامية التي يتسم بها الجاني أو النتيجة الإجرامية في جرائم تقنية المعلومات الماسة بأمن الدولة، وذلك من خلال تقريره لعقوبة وحيدة للجرائم على اختلاف أنواعها وهي عقوبة السجن المشدد.

المطلب الثاني: أركان جريمة تقنية المعلومات الماسة بأمن الدولة

نظرا للمسلك التشريعي الذي اتبعه كلا من المشرعين الإماراتي والمصري في مواجهة جرائم أمن الدولة المرتكبة بواسطة تقنية المعلومات، والذي يعتمد على النص على هذه الجرائم بحسب صورة السلوك الإجرامي المرتكب في كل منها، فان صور الركن المادي لهذا النوع من الجرائم تتعدد بحسب كل جريمة، وسواء وردت هذه الجريمة في المرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١، أو وردت في المرسوم بقانون اتحادي رقم ٣١ لسنة ٢٠٢١، أو غيرهم من القوانين طالما كان ارتكاب هذه الجريمة باستخدام احد وسائل تقنية المعلومات، وهو مناط اعتبارها احد جرائم تقنية المعلومات التي تستوجب تطبيق المرسوم بقانون رقم ٣٤ لسنة ٢٠٢١، كما هو الحال في القانون المصري الذي اعتبر ارتكاب أي من الجرائم الواردة في قانون العقوبات باستخدام تقنية المعلومات هو مناط لتطبيق القانون رقم ١٧٥ لسنة ٢٠١٨.

ومن استقراء مواد المرسوم بقانون رقم ٣٤ لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الإلكترونية نجد أن المشرع في المادة ٧١ قد نص على أن جرائم أمن الدولة هي الجرائم التي وردت في عدد من المواد الذي أوردها على سبيل الحصر من خلال سرد المواد التي نصت عليها، والتي بلغت عشرين مادة تبدأ بالمادة ٣ من المرسوم بينما تنتهي هذه المواد بالمادة ٥٥ من المرسوم، ثم اختتم المادة ٧١ بالحكم الاحتياطي الذي يعتبر كافة الجرائم الواردة من جرائم أمن الدولة اذا ارتكبت لحساب او مصلحة دولة أجنبية أو جهة غير مشروعة.

وتقع كل جريمة من جرائم أمن الدولة المنصوص عليها بالمادة ٧١ ضمن أحد الفئات التي حددها المشرع في المرسوم بقانون رقم ٣٤ لسنة ٢٠٢١، حيث يتضمن الفصل الأول من القانون فئة الجرائم الواقعة على تقنية المعلومات وتشمل الجرائم الواردة بالمواد ٣، ٥، ٧، ١١ فقرة ٣، ١٢ فقرة ٣، ١٣، ١٩، وتستهدف هذه الجرائم تقنية المعلومات ذاتها، والمتمثلة في "التقنيات المستخدمة في إنشاء ومعالجة وتخزين وتبادل واستخدام نظم المعلومات والبرامج المعلوماتية والمواقع الإلكترونية والشبكات المعلوماتية".

ويتمثل السلوك الإجرامي الوارد في المادة ٣ في اختراق الجاني لنظام معلوماتي حكومي، وذلك سواء كان الجاني لا يحق له دخول هذا الموقع، أو يحق له الدخول لكنه تجاوز الحدود الزمنية أو الموضوعية له، وذلك بتعمده دخول الموقع بصورة تتجاوز الصلاحيات الممنوحة له من قبل السلطة المعنية (الأحمد، ٢٠٢٠، ٢٣)[١٦]، بينما لم تحدد المادة ٥ سلوكا اجراميا بعينه، وانما عدت السلوك الإجرامي في جريمة الاضرار بالانظمة المعلوماتية الخاضعة للدولة هو أي سلوك يترتب عليه تدمير او تعطيل احد هذه الأنظمة بما يعني عدم قدرتها على تحقيق الغرض الذي وضعت من أجله بالصورة المعتادة، وتناولت المادة ٧ التعامل غير المشروع مع المعلومات والبيانات السرية المملوكة للدولة، وذلك عن طريق افعال الاتلاف والتعديل والاستحواذ والنشر واعادة النشر، وهو مسلك تشريعي يختلف عما ورد بالمادة ٥، اذ حدد المشرع صور السلوك الإجرامي على سبيل الحصر، الأمر الذي اتبعه ايضا من خلال المادة ١١ فقرة ٣ التي حددت السلوك الاجرامي في اصطناع موقع او بريد او حساب الكتروني على غرار ما هو مملوك للدولة، وكذلك ما اتبعه في المادة ١٢ فقرة ٣ حينما حدد السلوك الاجرامي في اعتراض اتصالات او معلومات او بيانات تخص احدى مؤسسات الدولة (شلتوت، ٢٠٢١، ١٠٤)[١٧]، والمادة ١٣ التي تناولت استخدام وسائل تقنية المعلومات في جمع بيانات ومعلومات تخص مواطني الدولة والمقيمين فيها، وبغض النظر عن الهدف من هذا الفعل، واخيرا يتجسد السلوك الاجرامي الوارد في المادة ١٩ في نشر اي محتوى يتعارض مع المعايير الصادرة من الجهات المختصة.

ويلاحظ على صور السلوك الاجرامي الخاصة بهذه الفئة من جرائم تقنية المعلومات الماسة بأمن الدولة ان المشرع عمد من خلال النص التشريعي الى تحديد السلوك الاجرامي بصورة دقيقة في أغلبها، حيث ربط السلوك الاجرامي بالنتيجة الاجرامية في المادة ٥ فحسب، والتي تناول الإضرار بالنظم المعلوماتية الحكومية، وهو الامر المفهوم في ظل خطورة هذا النوع من الجرائم والتي تستلزم تحديدا دقيقا لوصف السلوك الاجرامي فيها منعا لاي خلط قد يحدث فيتسبب في تكييف الجريمة بصورة على خلاف الواقع.

وتتجلى الفئة الثانية من جرائم تقنية المعلومات الماسة بأمن الدولة في جرائم المحتوى الالكتروني، وهي الجرائم المنصوص عليها في باقي المواد المذكورة في نص المادة ٧١، وتشمل ثلاثة عشر جريمة تبدأ بما نصت عليه المادة ٢٠ وهي جريمة الدعوة والترويج لتعطيل أحكام الدستور والقوانين، والسلوك الاجرامي في

هذه الجريمة هو انشاء او ادارة او الاشراف على موقع الكتروني، او النشر على هذا الموقع، بهدف تغيير نظام الحكم في الدولة، كما اختتم المشرع المادة ٢٠ بتجريم التحريض على هذه الأفعال، وهو ما يتبين منه تحديد المشرع لمظاهر السلوك الاجرامي والتي بينها في اربعة افعال بالاضافة للتحريض على والترويج لها.

واشتركت هذه الصور للسلوك الاجرامي لينص عليها المشرع في المادة ٢١ بخصوص الترويج للجماعات الارهابية، والمادة ٢٣ بخصوص التحريض على المساس بأمن الدولة والاعتداء على مأموري الضبط، والمادة ٢٤ التي تناولت الترويج لاثارة الفتنة والمساس بالوحدة الوطنية، والمادة ٢٦ التي واجهت الدعوة للتظاهر دون ترخيص، اذ اشتركت هذه المواد في ذات الركن المادي المتمثل في الانشاء والادارة والاشراف والنشر عبر وسائل تقنية المعلومات مع اختلاف الغرض من هذه الأفعال، بينما اختلف السلوك الاجرامي الوارد في المادة ٢٢، حيث تمثل في تقديم معلومات غير مصرح بتداولها او نشرها الى اي جهة اذا كان هذا التقديم من شأنه المساس بأمن الدولة والذي يتمثل في الاضرار بمصالحها او الاساءة اليها بأي صورة من الصور، ويستوي في هذا التقديم ان تكون المعلومات المنسوخة مسجلة على احد وسائل التخزين الالكترونية كالاسطوانات المدمجة او كروت الذاكرة، او كان عن طريق الارسال عبر البريد الالكتروني او احد الحسابات على مواقع التواصل الاجتماعي، حيث ان مناط تطبيق المادة ٢٢ هو ان يتم تقديم المعلومات المحظور تداولها عبر احد وسائل تقنية المعلومات (آل مواش، ٢٠١٧، ٥٢)[١٨].

بينما تمثل السلوك الاجرامي في فعل النشر في عدد من الجرائم المنصوص عليها في المرسوم بقانون رقم ٣٤ لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الالكترونية، ومنها ما نصت عليه المادة ٢٥ من تجريم نشر المواد المرئية او المسموعة او المقروءة التي تمثل سخرية او إضرار بسمعة الدولة، ويستوي في ذلك ان يكون النشر الالكتروني لمقال او صور مرسومة او تصميمات طالما كان من شأن المادة المنشورة ان تسئ لسمع الدولة، وهو ذات السلوك الاجرامي الذي نصت عليه المادة ٢٧ والتي حظرت نشر كل ما يمثل تحريض على الخروج على القانون وعدم الانصياع للقواعد التشريعية، سواء كانت هذه القواعد في الدستور او التشريع العادي او اللوائح المعمول بها في الدولة، وكذلك ما تضمنته المادة ٢٨ من حظر نشر اي مواد تسيء الى دولة اجنبية (سالمان، ٢٠٢٢، ١٣٦)[١٩]، واخيرا حظرت المادة ٥٢ نشر الشائعات وتداول الاخبار الزائفة، بالاضافة الى حظر نشر المواد التي تؤدي الى تأليب الرأي العام، بحيث تنطبق المادة ٥٢ بمجرد النشر حتى لو لم تتحقق أي نتيجة اجرامية بناء على هذا النشر (ريان، ٢٠٢٢، ١١٦)[٢٠].

وتستقل المادة ٤٧ بصورة السلوك المجرّم من خلالها وهو اجراء الاحصائيات والدراسات الاستطلاعية دون تصريح من السلطة المختصة بقصد الاضرار بمصالح الدولة، ولم تشترط المادة ان يتحقق الاضرار او التأثير بمصلحة الدولة، وانما يكفي ان يقوم الجاني بهذه الدراسات وهو يقصد تحقق هذا الضرر، كما تستقل المادة ٥٣ بسلوكها الاجرامي المتمثل في تخزين او اتاحة او نشر محتوى مخالف للقانون والامتناع عن ازالته

رغم صدور امر بذلك من السلطة المختصة، وهو سلوك ينقسم الى شق ايجابي تجسده افعال النشر والاتاحة والتخزين، وشق سلبي يتمثل في الامتناع عن ازالة المحتوى المحظور، واخيرا تناولت المادة ٥٥ فعل قبول العطية مقابل نشر محتويات غير قانونية او معلومات على خلاف الحقيقة، وهو الفعل الذي يعني تكراره قيام قرينة على ان الموقع الالكتروني في ذاته هو موقع مسئ، اما المشرع المصري فباعتباره ان المساس بأمن الدولة في الجرائم الالكترونية هو ظرف مشدد وليس جريمة لها ذاتيتها فإنه يقر ان كافة الجرائم التي يتصور ارتكابها بواسطة تقنيات المعلومات هي جرائم ماسة بأمن الدولة في حالة ارتكابها بقصد مما ورد في المادة ٣٤ من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، وهو ما يعني أن جرائم تقنية المعلومات الماسة بأمن الدولة هي جرائم لا تقبل الحصر في التشريع المصري، اذ ان مناط اعتبارها كذلك هو استهدافها لمقاصد بعينها على سبيل الحصر، وهي المقاصد الواردة في المادة ٣٤.

مما سبق يتبين أن المشرع الاتحادي في مسلكه تجاه تحديد صور السلوك الاجرامي لجرائم تقنية المعلومات الماسة بأمن الدولة اعتمد اساسا يختلف عن المشرع المصري، اذ نص على هذه الجرائم بصورة صريحة في المرسوم بقانون رقم ٣٤ لسنة ٢٠٢١، كما ضمن المرسوم حكما احتياطيا يجعل من الجرائم الواردة في المرسوم تحمل ذات الوصف في حالة تحقق وقائع مادية معينة، بينما اعتمد المشرع المصري في اعتباره جرائم تقنية المعلومات ماسة بأمن الدولة على القصد الجنائي لا الوقائع المادية، فعدها كذلك في حالة تحقق احد القصود الخاصة التي نص عليها في المادة ٣٤ من قانون مكافحة جرائم تقنية المعلومات المصري.

وتتعدد صور القصد الجنائي في جرائم تقنية المعلومات الماسة بأمن الدولة، فبينما اشترط المشرع الاماراتي تحقق قصد جنائي خاص في بعض الجرائم كشرط لقيام المسئولية الجنائية عنها، فانه قد اكتفى حيال جرائم اخرى بالقصد الجنائي العام، في الوقت الذي اشترط المشرع المصري فيه تحقق صورة او اكثر من صور القصد الجنائي الخاص كمناط لقيام المسئولية عن جرائم امن الدولة المرتكبة بواسطة وسائل تقنية المعلومات، وعلى هذا يمكن تصنيف جرائم تقنية المعلومات الماسة بأمن الدولة في التشريع الاماراتي من ناحية نوع القصد الجنائي الذي اشترط المشرع توافره الى جرائم ذات قصد جنائي عام وجرائم ذات قصد جنائي خاص.

اولا: الجرائم ذات القصد الجنائي العام: لم يشترط المشرع الاتحادي تحقق اي من صور القصد الجنائي الخاص بخصوص الجرائم الواقعة على تقنية المعلومات، حيث اكتفى في جميع الجرائم الواقعة تحت نطاق هذه الطائفة بالقصد الجنائي العام، عملا منه على اتساع نطاق التجريم وعدم السماح لأي عراقيل بالحيلولة دون تجريم هذه الأفعال، وضبط مرتكبيها وتقديمهم للمحاكمة، وذلك لما يتميز به مرتكبو هذه الجرائم من

خطورة اجرامية، وكذلك لخطورة النتائج المترتبة عليها والتي تصيب النظام المعلوماتي الحكومي ذاته وتهدد بالإضرار بما يتضمنه من معلومات (المردني، ٢٠٢٢، ٧٨)[٢١].

واولى هذه الجرائم هي جريمة اختراق النظم المعلوماتية الحكومية الواردة بالمادة ٣ من المرسوم بقانون رقم ٣٤ لسنة ٢٠٢١، وهي جريمة لم يحدد لها المشرع اي من صور القصد الخاص، فاكتفى بضرورة توافر القصد الجنائي العام بعنصريه العلم والإرادة، حيث يشترط ان يقدم الجاني على ارتكاب الجريمة وهو عالما بعناصرها الإجرامية والنتيجة التي تؤدي اليها، والتي تتمثل في ولوجه الى موقع الكتروني او نظام معلوماتي حكومي دون وجه حق، مع توافر ارادته الواعية المختارة في إتيانها رغم علمه بهذه العناصر، وهو ما ينطبق على ما ورد بالمادة ٥ وهي جريمة الإضرار بأنظمة المعلومات الحكومية، والتي تقوم عنها المسئولية الجنائية بمجرد تحقق الضرر على اي من الصورة المنصوص عليها بالمادة المذكورة، وهي التدمير والايقاف والتعطيل، وكذلك ما نص عليه في المادة ٧ وهي جريمة الاعتداء على المعلومات والبيانات التي يتضمنها النظام المعلوماتي الحكومي، وجريمة اصطناع المواقع الالكترونية والبريد الالكتروني والحسابات الزائفة لمواقع مملوكة للدولة التي نص عليها المشرع الاتحادي في المادة ١١ فقرة ٣ من المرسوم بقانون، وجريمة اعاقة او تعطيل الاتصالات الالكترونية الحكومية المنصوص عليها في المادة ١٢ فقرة ٣، وجريمة جمع المعلومات والبيانات الشخصية على خلاف القانون بالمادة ١٣، وجريمة نشر معلومات غير متوافقة مع معايير المحتوى الاعلامي الصادرة من السلطات المختصة بالمادة ١٩.

ويستمر المشرع الاماراتي على ذات النهج في اغلب جرائم المحتوى المعلوماتي، حيث يكتفي بضرورة تحقق القصد الجنائي العام كمناط لقيام المسئولية الجنائية عن ارتكاب هذه الجرائم، وهو ما يبدو في المادة ٢٠ التي تنظم الدعوة لتعطيل احكام الدستور والقوانين، والتي تقع فيها الجريمة بمجرد الدعوة الى التعطيل عن طريق احد وسائل تقنية المعلومات، دون اشتراط ان تهدف هذه الدعوة لتحقيق غرض بعينه، وجريمة نشر معلومات اضرارا بمصالح الدولة التي تقع بمجرد تقديم الجاني معلومات من شأنها تحقق هذا الإضرار الى أي جهة كما حددت المادة ٢٢، وما نصت عليه المادة ٢٣ من التحريض على المساس بأمن الدولة او الاعتداء على مأموري الضبط، وجريمة اثارة الفتنة والإضرار بالوحدة الوطنية في المادة ٢٤، والدعوة للتظاهر دون ترخيص في المادة ٢٦، وعدم الانقياد للتشريعات في المادة ٢٧، والإساءة لدولة اجنبية في المادة ٢٨، وجريمة نشر الشائعات والاخبار الكاذبة في المادة ٥٢، واتاحة المحتوى المخالف والامتناع عن ازالته رغم صدور امر بالازالة من السلطات المختصة وهو ما نصت عليه المادة ٥٣، واخيرا جريمة قبول عطية نظير نشر محتوى غير قانوني او معلومات زائفة والتي تقع بموجب المادة ٥٥ بمجرد تلقي هذه العطية حتى لو لم يتم النشر فعليا، وذلك دون اشتراط استهداف الجاني لأي غرض طالما كان من شأن هذا الإضرار بالدولة والاساءة لها (العتوم، ٢٠٢١، ١٨٨)[٢٢].

ثانيا: الجرائم ذات القصد الجنائي الخاص: اشترط المشرع الاماراتي تحقق احد صور القصد الجنائي الخاص كشرط لقيام المسئولية الجنائية عن هذه الجرائم، بحيث لا يكفي تحقق علم المتهم بعناصر الجريمة واتجاه ارادته لاتكابها، وهو الوضع الذي اقتصر في المرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الالكترونية في ثلاثة مواد هي ٢١، ٢٥، ٤٧ فقرة ٢، وتنظم المادة ٢١ جريمة التحبيذ والترويج للجماعات الارهابية، وهي مظاهر السلوك الاجرامي التي اشترط المشرع ان تقترن بهدف تسهيل الاتصال بين افراد الجماعة وقاداتها، او استقطاب اعضاء للانضمام للجماعة، او نشر افكارها والترويج لهذه الأفكار، او تمويل الانشطة او تقديم مساعدة للجماعة، وأخيرا ان يكون التحبيذ عن طريق نشر طرق تصنيع المواد المحظورة كالمتفجرات والأسلحة والأدوات التي تستعمل عادة في ارتكاب الجرائم الإرهابية (عبد المطلب، ٢٠٢٢، ٦٩)[٢٣].

كما تتصدى المادة ٢٥ لجريمة الاضرار بسمعة الدولة والسخرية منها، وهي الجريمة التي اشترط المشرع لتحققها وجود قصد جنائي خاص يتمثل في قصد الاضرار بسمعة الدولة او النيل من هيبتها او السخرية من رموزها او سلطاتها او مؤسساتها، بحيث تحقق المسئولية الجنائية في حالة اقدام الجاني على نشر اي من المواد المقروءة او المسموعة او المرئية عبر وسائل تقنية المعلومات مع استهدافه لأي من هذه المقاصد التي وردت على سبيل الحصر في المادة ٢٥.

واخيرا تتناول الفقرة الثانية من المادة ٤٧ جريمة اجراء الدراسات الاستطلاعية والاحصائيات دون تصريح من السلطات الحكومية المختصة اذا قصد من هذه الاستطلاعات وجمع الاحصائيات الاضرار بمصالح الدولة والتأثير في هذه المصالح، بحيث تنتفي المسئولية الجنائية اذا كان الهدف من القيام بهذه الاستطلاعات هو هدف مغاير للاضرار بمصلحة الدولة، كابتغاء الجاني تحقيق هدف علمي، او ممارسته لهواية معينة، او العمل على دراسة حالة المجتمع تمهيدا للاقدام على احد المشروعات التجارية، حتى لو كانت هذه الاستطلاعات قد تمت في غيبة موافقة السلطات المختصة ومنحها الترخيص اللازم للجاني.

وعلى هذا يتبين أن المشرع الاماراتي قد اكتفى بتحقق القصد الجنائي العام المتمثل في العلم والاراد من خلال السواد الأعظم من المواد التي تنظم جرائم تقنية المعلومات الماسة بأمن الدولة، وهو الأمر المفهوم حيث تعد هذه الجرائم مما يشكل خطورة على المجتمع بصورة كبيرة، مما يستوجب من المشرع تيسير عملية تجريمها، والتوسع في العقاب عليها، الأمر الذي يتنافي مع اشتراط تحقق قصد جنائي خاص.

وبرغم ندرة الجرائم التي نص فيها المشرع على ضرورة تحقق احد صور الجنائي الخاص الا ان الباحث كان يأمل ان يعدل المشرع الاتحادي عن مسلكه الذي تضمنته المادة ٢١ من المرسوم بقانون رقم ٣٤ لسنة ٢٠٢١، فيكتفي بتحقق القصد الجنائي العام لقيام المسئولية الجنائية عن الترويج للجماعات الارهابية، اذ ان فعل الترويج والتحبيذ ذاته يعد من مظاهر السلوك الاجرامي التي تتسم بالخطورة الشديدة حتى لو لم تقترن

بأحد صور القصد المنصوص عليها في المادة ٢١، كما أن الجاني حينما يرتكب افعال الترويج والتحبيذ انما يقوم بذلك وهو مؤمن بالعقائد الفكرية لهذه الجماعات، وبالتالي هو إما احد اعضائها او مشروع عضو من اعضائها، الأمر الذي يستوجب معاملته بالشدة الواجبة دون النظر عن مقصده من ارتكاب افعال الترويج والتحبيذ.

أما المشرع المصري فنظرا للمسلك التشريعي الذي اتخذه من خلال القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات فقد عد كافة الجرائم الواردة في هذا القانون والماسة بأمن الدولة هي من الجرائم التي تتطلب وجود قصد جنائي خاص، وهو ما كرّس له من خلال المادة ٣٤ من القانون والتي عددت صور القصد الجنائي الخاص اللازمة لاعتبار جريمة تقنية المعلومات احدى الجرائم الماسة بأمن الدولة، حيث حصرتها في تعريض أمن وسلامة المجتمع للخطر، او الاخلال بالنظام العام، او الإضرار بالأمن القومي للدولة، او مركزها الاقتصادي، او تعطيل احكام الدستور او القوانين او اللوائح، او عرقلة او منع السلطات العامة في الدولة عن ممارسة اختصاصاتها، او الإضرار بالسلام الاجتماعي او الوحدة الوطنية.

المبحث الثاني: المواجهة الجزائية لجرائم تقنية المعلومات الماسة بأمن الدولة

تمهيد وتقسيم:

اتبع كلا من المشرعين الاماراتي والمصري مسلكا تشريعيا يتسم بالتشديد في العقاب إزاء جرائم تقنية المعلومات الماسة بأمن الدولة، وهو الأمر الذي فرضه واقع هذه النوع من الجرائم والتي تستهدف الإضرار بمصالح الدولة العليا "وفداحة الأضرار التي قد تنتج عن مثل هذه الجرائم التي قد يترتب عليها انهيار مجتمعات إنسانية بأكملها" (السويدي، ٢٠١٥، ٧٥)[٢٤]، الأمر الذي يوضح أسباب التشديد العقابي تجاه هذا النوع من الجرائم.

وبمقارنة مسلكي كلا من المشرعين الاماراتي والمصري نجد أن اتجاه المشرع الاتحادي قد نص على العديد من العقوبات بعكس المشرع المصري الذي اختصر سياسته الجزائية في عقوبة واحدة، وهو الأمر المفهوم نظرا لاعتبار الجرائم الواردة في المرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١ هي جرائم ماسة بأمن الدولة لها ذاتيتها واستقلالها، بينما جائت الجرائم المنصوص عليها في القانون رقم ١٧٥ لسنة ٢٠١٨ كجرائم تقليدية يعد مساسها بأمن الدولة مجرد ظرف مشدد، مما يترتب عليه وحدة العقوبة التي تترتب على هذا التشديد.

واذا كان هناك اختلاف في السياسة العقابية بين كلا من التشريعين الاماراتي والمصري، فإن هذا الاختلاف قد ظهر أثره ايضا في النظام الاجرائي لجرائم تقنية المعلومات الماسة بأمن الدولة في كلا من

قانوني الاجراءات الجزائية في الدولتين، فبينما افرد المشرع الاماراتي نصوصا قانونية خاصة بالجرائم الماسة بأمن الدولة، ترك المشرع المصري هذا التنظيم للقواعد العامة في قانون الاجراءات الجنائية.

المطلب الأول: العقوبة المقررة فى ضوء القانون الإماراتي والمصري.

المطلب الثاني: إجراءات جمع الاستدلالات والتحقيق فى جرائم تقنية المعلومات الماسة بأمن الدولة.

المطلب الأول: العقوبة المقررة فى ضوء القانون الإماراتي والمصري

اتبع المشرع الاماراتي مبدأ التدرج العقابي في جرائم تقنية المعلومات الماسة بأمن الدول، حيث جمعت احكامه بين العقوبات السالبة للحرية والعقوبات المالية، كما تنوعت العقوبات السالبة للحرية بين الحبس والسجن المؤقت والسجن المؤبد في الوقت الذي اقتصرت فيه احكام التشريع المصري على السجن المشدد.

وتتمثل العقوبات الأصلية في المرسوم بقانون رقم ٣٤ لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الالكترونية في الحبس والسجن المؤقت والسجن المؤبد بالاضافة للعقوبات المالية، حيث قرر المشرع الاتحادي عقوبة الغرامة المالية على جريمة واحدة، وهي الجريمة المنصوص عليها في المادة ٥٣ وهي اتاحة محتوى قانوني للاطلاع والامتناع عن ازالته رغم صدور امر بذلك من الجهات المختصة، فقرر عقوبة الغرامة التي تتراوح بين ثلاثمة الف درهم وعشرة ملايين درهم، في تباعد واضح بين الحدين الادنى والاقصى للعقوبة يسمح للقضاء بالتفريد القضائي بصورة كبيرة (لطفي، ٢٠٢١، ٣٩)[٢٥].

كما جمع المشرع بين عقوبتي الحبس والغرامة على سبيل الالزام او التخيير في عدد من الجرائم، حيث عاقبت المادة ١١ فقرة ٣ بالحبس بحد اقصى ٥ سنوات والغرامة التي تتراوح بين مائتي الف ومليوني درهم على جريمة اصطناع موقع او حساب الكتروني ونسبه زورا لاحد مؤسسات الدولة، كما قررت المادة ٢٥ ذات العقوبة السالبة للحرية بينما نزلت بالحد الاقصى للغرامة المالية على جريمة السخرية من الدولة ورموزها والاساءة لهم عبر النشر على وسائل تقنية المعلومات، اما المادة ٢٦ فقد عاقبت بالحبس والغرامة التي تتراوح بين مائتي الف ومليون درهم او احدى هاتين العقوبتين لجريمة التحريض على التظاهر دون ترخيص مسبق من الجهات المعنية، وهي ذات عقوبة جريمة التحريض على عدم الانقياد للتشريعات والمنصوص عليها بموجب المادة ٢٧ مع النزول بالحدود الدنيا والقصوى للغرامة المالية الى مائة الف درهم كحد ادنى وخمسمائة الف درهم كحد اقصى مع منح القضاء سلطة التخير بين العقوبة السالبة للحرية والعقوبة المالية، كما عاقبت المادة ٢٨ على جريمة الاساءة لدولة اجنبية بالحبس مدة لا تقل عن ستة أشهر والغرامة التي تتراوح بين مائة الف وخمسمائة الف درهم او احدى هاتين العقوبتين، وعاقبت المادة ٥٢ على نشر الشائعات الكاذبة بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن مائة الف درهم مع رفع العقوبة الى سنتين ومائتي الف درهم في حالة نتج عن نشر الشائعات تأليب الرأي العام وحالة القيام بالنشر في حالات الطوارئ المتمثلة في الاوبئة والازمات والكوارث.

وأخيرا قرر المشرع الاتحادي عقوبة السجن المؤقت لعدد أخر من الجرائم الواردة بالمرسوم اتحادي رقم ٣٤ لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الالكترونية، حيث نصت المادة ٣ على عقوبة السجن المؤقت والغرامة التي تتراوح بين مائتي الف وخمسمائة الف درهم لجريمة اختراق المواقع الالكترونية الحكومية، بينما نصت المادة ٥ على عقوبة السجن المؤقت والغرامة التي تتراوح بين خمسمائة الف وثلاثة ملايين درهم لجريمة الاعتداء على نظام معلوماتي حكومي، وتشدد المادة ٧ العقوبة لتجعل الحد الادنى للسجن المؤقت ٧ سنوات مع الابقاء على الحدود الدنيا والقصوى للعقوبة المالية الواردة بالمادة ٥ وذلك لجريمة الاعتداء على البيانات والمعلومات الحكومية، مع رفع الحد الادنى للسجن المؤقت الى ١٠ سنوات والحد الاقصى للغرامة الى خمسة ملايين درهم في حالة نتج عن الاعتداء فقدان سرية المعلومات او الانظمة او الاتصالات الخاصة بالمنشآت العسكرية او الأمنية، والاكتفاء بالسجن المؤقت دون عقوبة مالية في حالة تخزين هذه المعلومات مع العلم بعدم مشروعية الحصول عليها.

كما تقرر المادة ١٢ فقرة ٣ عقوبة السجن المؤقت لجريمة اعتراض الاتصالات او المعلومات والبيانات التابعة لاحدى مؤسسات الدولة، وقررت المادة ٢١ عقوبة السجن مدة تتراوح بين عشر سنوات وخمسة وعشرين سنة والغرامة التي تتراوح بين مليوني درهم واربعة ملايين درهم لجريمة الترويج للجماعات الارهابية، كما عاقبت المادة ٢٢ بالسجن المؤقت كل من ينشر معلومات للاضرار بمصلحة الدولة، بينما عاقبت المادة ٢٣ بالسجن المؤقت والغرامة التي لا تزيد عن مليون درهم على التحريض على المساس بأمن الدولة ومأموري الضبط القضائي، وهي ذات العقوبة التي قررتها المادة ٢٤ لجريمة الترويج لاثارة الفتنة الطائفية مع تقرير حد ادنى للغرامة يتمثل في مائتي الف درهم، واخيرا قررت المادة ٥٥ عقاب من يتلقى مقابلا لقاء نشر محتوى غير قانوني او معلومات زائفة بالسجن المؤقت والغرامة التي لا تزيد عن مليوني درهم، وقرر المشرع الاتحادي عقوبة السجن المؤبد لجريمة وحيدة هي جريمة الترويج لتعطيل احكام الدستور والقوانين، وهي الجريمة الواردة بالمادة ٢٠ من المرسوم بقانون رقم ٣٤ لسنة ٢٠٢١، حيث تعد هذه الجريمة هي أخطر الجرائم الواردة بالمرسوم لوقوعها على النظام الدستوري للبلاد، مع معاقبة الشريك في هذه الجريمة بذات عقوبة الفاعل الأصلي (حسن، ٢٠٢١، ١٠٩)[٢٦].

وبرغم نص المادة ٧٢ على ان تطبيق المرسوم بقانون رقم ٣٤ لسنة ٢٠٢١ لا يخل بتطبيق أي عقوبة اشد قد ترد في اي قانون لآخر، الا ان خلو هذا المرسوم بقانون من عقوبة الاعدام يثير التساؤل، خاصة مع الذاتية التي منحه المشرع اياها باعتبارها القانون الوحيد الذي ينظم جرائم تقنية المعلومات، وكان الأحرى بالمشرع ان يحافظ على هذه الذاتية فيكفل لهذا القانون التطبيق دون الرجوع لأي قانون آخر باعتباره يقر لهذا القانون بالاختصاص بتنظيم جرائم تقنية المعلومات بصورة عامة، أما المشرع المصري فقد تفرد بموقف يراه الباحث استثنائيا، إذ نص على عقوبة أصلية وحيدة لكافة جرائم أمن الدولة المنصوص عليها في القانون رقم

١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، وهي السجن المشدد في حالة ارتكاب أي جريمة من هذه الجرائم، وهو ما نصت عليه المادة ٣٤ من القانون رقم ١٧٥ لسنة ٢٠١٨.

اما عن الظروف المشددة فقد كان المشرع الاتحادي واضحا دقيقا في تحديد الظروف المشددة في جرائم تقنية المعلومات الماسة بأمن الدولة والمنصوص عليها في المرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الالكترونية، حيث حددت المادة ٦٠ هذه الظروف على سبيل الحصر، وهي العوامل التي يؤدي توافرها الى تعديل العقوبة بالتغليظ، وذلك بحسب القواعد العامة الواردة في المادة ١٠٤ من المرسوم بقانون رقم ٣١ بإصدار قانون الجرائم والعقوبات، والتي تتمثل في مضاعفة الحد الأقصى للغرامة او الحكم بالحبس عوضا عنها في حالة كانت العقوبة الأصلية هي الغرامة، ومضاعفة الحد الاقصى للحبس في حالة كانت العقوبة الأصلية هي الحبس، والوصول بمدة السجن المؤقت الى ١٥ سنة في حالة كانت العقوبة المقررة السجن المؤقت الذي يقل عن هذه المدة، وأخيرا الحكم بالسجن المؤبد اذا كان الحد الاقصى للعقوبة المقررة هي السجن المؤقت بحده الأقصى، ويقتصر إعمال التشديد على هذه الحالات الواردة على سبيل الحصر، فلا يجوز إعماله في حال كان الحد الاقصى للعقوبة هو السجن المؤبد، اذ يملك القاضي ان يحكم بالسجن المؤبد في هذه الحالة بما لا يدع هناك مجالا للتشديد (عبد العاطي، ٢٠٢١، ٧٥)[٢٧].

وفي تناول المشرع للظروف المشددة من خلال المادة ٦٠ قرر ان هذه الظروف هي ارتكاب الجني للجريمة بسبب او بمناسبة تأديته لعمله، وارتكابه للجريمة لحساب او مصلحة دولة أجنبية او جماعة ارهابية او جماعة معادية او تنظيم غير مشروع، وهي حالات تضفي مزيد من الخطورة الاجرامية على شخصية الجاني كما تسفر عن نتائج اجرامية اكثر فداحة، حيث يعبر استغلال الموظف للسلطات الممنوحة له بموجب وظيفته لارتكاب جريمة ماسة بأمن الدولة عن خيانة هذا الجاني للأمانة التي حملته الدولة والمجتمع اياها، كما أن كون الجاني احد الموظفين العموميين يجعل منه اكثر قدرة على ارتكاب هذا النوع من الجرائم نظرا للسلطات المخولة له، ولمعرفته بأسرار الوظيفة والأسلوب الأمثل لارتكابها، كما يمنحه فرصة أكبر من غيره لاخفاء معالم جريمته مما يصعب ضبطها والكشف عن مرتكبها ومعاقبته طبقا لأحكام القانون (خضر، ٢٠٢٢، ٨٨)[٢٨].

ويفترض إعمال هذا التشديد كون الجاني موظفا عاما، وارتكابه للجريمة بسبب او مناسبة أعماله الوظيفية، بحيث يؤدي انتفاء تحقق أحد الشرطين الى انتفاء مناط التشديد وتوقيع العقوبة في صورتها البسيطة، وهو ما يتصور حينما يرتكب الموظف العام أحدى الجرائم المنصوص عليها دون أن يستند لوظيفته كعامل مساعد على ارتكاب الجريمة، او بعيدا عن اختصاصه او سلطاته الوظيفية، الأمر الذي يجعل منه شخصا عاديا إزاء هذه الجريمة (علام، ٢٠١٦، ١٠٨)[٢٩]، مما يستوجب تطبيق القواعد العامة في العقاب دون إعمال التشديد الوارد بالمادة ٦٠ من المرسوم بقانون رقم ٣٤ لسنة ٢٠٢١.

أما الظرف المشدد الثاني الذي قرره المشرع الاتحادي في جرائم تقنية المعلومات الماسة بأمن الدولة فهو حالة ارتكاب الجاني لجريمته مدفوعا بالعمل لصالح او لحساب دولة اجنبية، او جماعة ارهابية، او جماعة معادية، او تنظيم غير مشروع، وهو الظرف الذي سعى المشرع الاتحادي من خلاله الى حصر كافة الجهات التي يمكن ان يعمل الجاني لحسابها، بحيث تشمل المادة كافة احتمالات العمل لحساب الجهات الخارجية، سواء كانت جهات تملك الشخصية الاعتبارية كالدول الاجنبية، او جهات تمثل جماعات او تنظيمات غير مشروعة.

ولا يتعدى اثر التشديد في هذه الحالة من ينطبق عليه التشديد دون ان يمتد لغيره من الفاعلين او الشركاء في الجريمة، فإذا جمعت الجريمة بين موظف عمومي واخرين وارتكبت بمناسبة او بسبب الوظيفة التي يشغلها هذا الموظف فيعد الظرف المشدد ظرفا خاصا به دون غيره من الفاعلين.

اما على صعيد التشريع المصري فبالرغم من افراده نصوصا خاصة لتنظيم الجرائم الماسة بأمن الدولة من خلال قانون العقوبات المصري، الا انه لم يتخذ ذات المسلك ضمن نصوص القانون رقم ١٧٥ لسنة ٢٠٢١، فعد السمات التي تحيل الجريمة الى جريمة ماسة بأمن الدول هي من قبيل الظروف المشددة، فقررت المادة ٣٤ من هذا القانون ان تحقق احد الحالات الواردة فيها يعد مناطا لتشديد العقوبة المقررة لأي جريمة مما ورد بالقانون، مما يستوجب الحكم على الجاني بالسجن المشدد أي كانت الجريمة المرتكبة.

والواقع ان هذا المسلك يتعارض مع طبيعة العقوبات المقررة من خلال مواد هذا القانون، اذ يتضمن النص على عدد من الجرائم التي لا تزيد عقوبتها عن الحبس بحد اقصى ثلاثة أشهر مثل جريمة الانتفاع بدون وجه حق بالنظام المعلومات، والواردة بالمادة ١٣ من القانون، كما يتضمن عقوبة الحبس مدة لا تقل عن سنتين والمقررة بموجب المادة ١٧ لجريمة الاعتداء على سلامة النظم المعلوماتية، وفي المقابل يشمل عقوبة السجن المقررة بموجب المادة ٢٠ والخاصة بجريمة اعتراض البيانات الحكومية او الحصول عليها دون وجه حق، وبالرغم من هذا التفاوت في تكييف الجرائم المنصوص عليها في هذا القانون والتي تتراوح بين الجنح والجنايات، مما يقابله تفاوت في العقوبات بين الحبس البسيط والسجن، الا ان العقوبة على كافة الجرائم تتحول الى السجن المشدد وهو اقصى عقوبة سالبة للحرية في النظام الجنائي المصري في حالة تحقق احد الظروف المشددة، الأمر الذي يدعو للتساؤل عن مركز التدرج العقابي في القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات (سويلم، ٢٠١٩، ١٨٢)[٣٠].

مما سبق يتبين أن المشرع المصري لم يأخذ بمبدأ التدرج العقابي بالنسبة لجرائم تقنية المعلومات الماسة بأمن الدولة، اذ تعامل مع كافة الجرائم من هذا النوع على انها فئة واحدة مقررا لها عقوبة السجن المشدد، وهو تشديد نرى انه لم يكن في محله، اذ بينما شدد العقوبة من السجن للسجن المشدد في حالات، فانه قد غلظ من عقوبة بعض الجنح لتصل الى هذا الحد، وذلك على الرغم من كون أغلب الجرائم الواردة في القانون

رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات هي من الجنح التي تستوجب الحبس ثلاث سنوات.

المطلب الثاني: إجراءات جمع الاستدلالات والتحقيق فى جرائم تقنية المعلومات الماسة بأمن الدولة

لا يمكن إعمال المواجهة التشريعية لأي ظاهرة اجرامية من خلال القواعد الموضوعية بمفردها، إذ يستلزم نجاح هذه المواجهة وجود نظام اجرائي واضح يسمح بتفعيل اجراءات الاستدلال والتحقيق والمحاكمة بصورة تعين على ضبط الجرائم والكشف عن مرتكبيها وتقديمهم للمحاكمة من ناحية، كما يكفل كافة حقوق المتهمين في ابداء دفاعهم ودفوعهم في محاكمات عادلة ناجزة.

وبالحديث عن النظام الاجرائي لجرائم تقنية المعلومات الماسة بأمن الدولة نجد أن المشرع الاماراتي قد خصّ هذه الجرائم بعدد من الاجراءات واجبة الاتباع في مرحلتي الاستدلال والتحقيق، والتي يتميز بها النظام الاجرائي لهذه الجرائم عن القواعد العامة للنظم الاجرائية، في الوقت الذي اختلف فيه مسلك المشرع الاجرائي المصري والذي تعامل مع هذا النوع من الجرائم وفقا للقواعد العامة الواردة في قانون الاجراءات الجنائية دون أن يختصها بأي قواعد استثنائية، وهو الأمر الذي يفسره وجود نظام اجرائي خاص لجرائم امن الدولة في التشريع الاماراتي هو القانون رقم ٢ لسنة ٢٠٠٣ بشأن جهاز أمن الدولة، والذي يحدد المعاملة الاجرائية لهذا النوع من الجرائم بشكل يتلائم مع خطورتها والسرعة المطلوبة لضبطها ونسبها الى مرتكبيها.

وقررت المادة ٣٠ من قانون الاجراءات الجزائية الاتحادي اختصاص مأموري الضبط القضائي بمهمة جمع الاستدلالات في انواع الجرائم كافة، بما في ذلك جرائم تقنية المعلومات الماسة بأمن الدولة، كما حددت المادة ٣٣ مأموري الضبط ويأتي على رأسهم الضباط وصف الضباط والأفراد من جهاز الشرطة وباقي الأجهزة الأمنية (السويدي، ٢٠١٥، ٩٠)[٣١]، أما الاختصاص النوعي بضبط هذه الجرائم فيخضع للعاملين بجهاز أمن الدولة الاماراتي، وهو اختصاص نوعي ومكاني شامل في كل ما يخص الجرائم الماسة بأمن الدولة.

وقد منح القانون رقم ٢ لسنة ٢٠٠٣ بشأن جهاز أمن الدولة عامليه عددا من الصلاحيات الاستثنائية، تضمنتها المادتان ١٤، ٢٤ من القانون، وتتمثل في كشف الهوية، وتفتيش الاشخاص، وتفتيش الأماكن السكنية وغير السكنية، وحجز الاشخاص والتحفظ عليهم، وهي الصلاحيات التي تتسم بالخطورة الشديدة، والتي تتطلب حرص عند تطبيقها لانها تمنح الضبط الجنائي صلاحيات سلطة التحقيق في عدد من الحالات.

اولا: كشف الهوية: يهدف هذا الاجراء الى استيضاح شخصية المشتبه به والاستيثاق منها، كما يتضمن هذا الاستيضاح مهنته وعنوانه والمعلومات الخاصة بسلوكه، وهي سلطة تمنح لمديري الادارات في حالة

الاشتباه في ارتكاب المشتبه به لاحد الأنشطة الواردة في المادة ١٤ من القانون، كما يجوز لمدير الادارة تفتيش المشتبه به في هذه الحالة، والتحقيق معه، وحجزه (عبدول، ٢٠٠٧، ١٢)[٣٢].

ثانيا: تفتيش الأشخاص والأماكن: خرج المشرع عن القواعد العامة في قانون الاجراءات الجزائية بالنسبة لاجراء التفتيش سواء مس الاجراء الاشخاص او الاماكن في الجرائم الماسة بأمن الدولة، حيث منح رئيس الجهاز ونائبه سلطة اصدار الإذن الكتابي بتفتيش الاشخاص، وهي سلطة ممنوحة في الأصل لسلطات التحقيق، الا ان المشرع لاعتبارات الملائمة التي ترتبط بخطورة الجرائم الماسة بأمن الدولة قد منحها لمأمور الضبط الجنائي، شريطة ان تتوافر دلائل جدية على أن المشتبه به يحوز ما يفيد في كشف الحقائق الخاصة بالجريمة المتحرى عنها.

كما أجاز لرئيس الجهاز ونائبه اصدار اذن تفتيش الاماكن واستيضاح شخصيات المتواجدين بها، اذا توافرت دلائل جدية على وجود اشخاص او اشياء يجب ضبطها في هذه الاماكن، وسواء كان المكان من المحال العامة او المساكن، او دلائل على أن هناك اعتداء وشيكا على أمن الدولة او اعتداء قد وقع بالفعل او لأي ضرورة يستلزمها التحقيق في الجريمة بحسب المادة ٣٠ من القانون الاتحادي رقم ٢ لسنة ٢٠٠٣ في شأن إنشاء جهاز أمن الدولة.

ثالثا: حجز الاشخاص والتحفظ عليهم: يعد حجز الاشخاص والتحفظ عليهم من صلاحيات سلطات التحقيق والتي منحها المشرع للعاملين بجهاز أمن الدولة فيما يخص الجرائم الماسة بأمن الدولة، وذلك مع التمييز في مدة الحجز بحسب وظيفة مأمور الضبط، حيث منح مدير الادارة سلطة حجز الاشخاص لمدة أربع وعشرين ساعة، والمدير العام مدة ثمان وأربعين ساعة، ونائب رئيس الجهاز مدة اثنين وسبعين ساعة، بينما منح رئيس الجهاز سلطة حجز الأشخاص لمدة ستين يوما، وله صلاحية مدها الى تسعين يوما في حالة تعذر عرض المشتبه به على النيابة العامة، وقد وضع المشرع عدد من الضوابط التي تقيد هذا الاجراء، اهمها مدة الحجز والتي تتراوح بحسب منصب مأمور الضبط الذي يأمر به، وضرورة توافر أسباب جدية تحمل على الاعتقاد بارتكاب المشبه به أحد الأنشطة الواردة في المادة ١٤ من القانون، وأهمها الجرائم الماسة بأمن الدولة والأنشطة الإرهابية.

وعلى عكس التشريع الاماراتي الذي منح سلطات جمع الاستدلال عدد من الصلاحيات الاستثنائية إزاء الجرائم الماسة بأمن الدولة، التزم المشرع المصري بالقواعد العامة الواردة في قانون الاجراءات الجنائية بصورة مطلقة، فلم يفرد لجرائم امن الدولة اي نصوص اجرائية استثنائية، مما يعني التزام مأمور الضبط في مصر بما يلزمه به القانون تجاه كافة انواع الجرائم بما في ذلك الجرائم الماسة بأمن الدولة، وذلك على اعتبار وحدة النظام الاجرائي في مصر بالنسبة لكافة انواع الجرائم الخاضعة لاختصاص القضاء العادي.

الخاتمة

على الرغم من أن تقنيات المعلومات كان لها الأثر الأبرز خلال العقدين الأخيرين في تطوير الحياة الانسانية للأفضل بصورة عامة، الا ان الامر لم يخل من وجه سلبي اتسمت به هذه التقنيات كان أهمه دورها في تطوير الجريمة سواء باستحداث صور جديدة من الجرائم او حتى تطوير سبل ارتكاب الجرائم التقليدية، وهو الأمر الذي استوجب مواجهة هذه الظواهر الاجرامية الجديدة بموجب سياسة تشريعية متطورة تلائم التطور التقني الذي طرأ على الظاهرة الإجرامية.

وقد تصدى المشرعان الاماراتي والمصري لجرائم أمن الدولة من خلال هذين التشريعين بصورة يمكن الحكم بايجابيتها، حيث لجأ المشرع من خلال كلا منهما الى تقديم مفهوم قانوني لهذه الجرائم تم من خلاله توضيح صور السلوك الاجرامي وصور القصد الجنائي والتي تعد مناط قيام المسئولية الجنائية عن هذه الجرائم، كما حرص كل مشرع على تضمين القانون عدد من العقوبات التى رأى كفايتها لمواجهة جرائم تقنية المعلومات الماسة بأمن الدولة، برغم اختلاف السياسة الجنائية لدى كلا من المشرعيّن، وهو ما ترتب عليه اختلاف صور السلوك الإجرامي، واختلاف العقوبات فيما بينهما، الا أن الواقع القانوني يشهد بأن المشرع عادة ما يلجأ للتعديلات التشريعية بصورة مستمرة لاستكمال ما بالتشريع من نقص وذلك بعد تقييم اوجه القصور التي تبدو بالتطبيق العملي للتشريع، وهو ما يمنح الفرصة لتفعيل سبل المواجهة بصورة دائمة.

النتائج

١. اعتبر المشرع الاتحادي جرائم تقنية المعلومات الماسة بأمن الدولة جرائم مستقلة لها ذاتيتها من خلال المادة ٧١ من المرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الالكترونية، بينما تعامل المشرع المصري مع مساس جرائم تقنية المعلومات بأمن الدولة على إنه ظرف مشدد لجرائم تقنية المعلومات وذلك من خلال المادة ٣٤ من قانون مكافحة الجرائم الالكترونية رقم ١٧٥ لسنة ٢٠١٨.

٢. خرج المشرع الاتحادي عن القواعد العامة في التدرج العقابي في جرائم امن الدولة المرتكبة بواسطة تقنيات المعلومات فسوى بين العقوبة المقررة للشروع والفعل التام في احيان وقرر للشروح في الجنح نصف عقوبة الفعل التام في احيان اخرى، بينما تمثل خروج المشرع المصري عن هذه القواعد بنصه على عقوبة واحدة لكافة جرائم امن الدولة التي تقع باستخدام هذه الوسائل وهي السجن المشدد.

٣. قرر المشرع الاتحادي ظرفين مشددين في جرائم تقنية المعلومات الماسة بأمن الدولة، الأول هو ارتكاب الجاني لجريمته بسبب او بمناسبة وظيفته، والثاني هو ارتكابها لحساب دولة اجنبية او تنظيم غير مشروع، بينما اقتصر اتجاه المشرع المصري على اعتبار مساس جريمة تقنية المعلومات بأمن الدول هو ظرف مشدد في حد ذاته.

التوصيات

١. تعديل المادة ٢٧ من المرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الالكترونية ليصبح عنوان المادة " التحريض على عدم الانقياد للقوانين"، بحيث يشمل المعنى القواعد الدستورية والتشريعية واللوائح المعمول بها في الدولة، حيث ان عنوان المادة يوحي باقتصارها على مواجهة التحريض على عدم الانقياد للتشريع بمفهومه الضيق.

٢. تعديل المادة ٢٠ من قانون مكافحة الجرائم الالكترونية المصري رقم ١٧٥ لسنة ٢٠١٨ بحيث تنص على اعتبار الجرائم الواردة بالمادة من الجرائم الماسة بأمن الدولة بغض النظر عن الهدف من ارتكاب هذه الجرائم، حيث انها جرائم تقع على المصالح العليا للدولة بما يستوجب اعتبارها مساسا بالأمن القومي حتى لو أتت خالية من أي من صور القصد الجنائي الخاص.

٣. الغاء المادة ٣٤ من قانون مكافحة الجرائم الالكترونية المصري رقم ١٧٥ لسنة ٢٠١٨ واضافة التشديد الملائم لكل جريمة من خلال المادة التي نصت عليها، بحيث يتم مراعاة طبيعة ودرجة الخطورة المترتبة على كل جريمة بصورة مستقلة.

قائمة المراجع

١. أحمد زكي محمد عبد المطلب، جرائم التنظيمات الإرهابية وسبل مواجهتها – دراسة مقارنة، مركز الدراسات العربية للنشر والتوزيع، القاهرة ٢٠٢٢.

٢. أحمد غانم سيف السويدي، المواجهة الجنائية والأمنية للجرائم الماسة بأمن الدولة الداخلي، رسالة ماجستير، اكاديمية شرطة دبي، ٢٠١٥.

٣. احمد غانم سيف السويدي، مرجع سابق.

٤. أحمد غانم سيف السويدي، مرجع سابق.

٥. بخاري جميل علي، جريمة الإرهاب الدولي ومشروعية حركات النضال الوطني، المركز العربي للدراسات والبحوث العلمية، القاهرة ٢٠٢٠.

٦. بهاء المري، مكافحة جرائم تقنية المعلومات وحجية الدليل الرقمي في الإثبات، دار مصر للنشر والتوزيع، القاهرة ٢٠١٩.

٧. حاتم احمد بطيخ، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات، بحث منشور في مجلة الدراسات القانونية والاقتصادية، مجلد ٧ عدد ١، القاهرة ٢٠٢٠.

٨. حمدان أحمد إبراهيم البلوشي، التدابير الأستباقية لمواجهة التطرف الفكري الإرهابي في التشريع الإماراتي – دراسة مقارنة، المتحدة للنشر والتوزيع، ابوظبي ٢٠٢٢.

٩. حمدة خلفان منصوري، الجرائم الإلكترونية الماسة بأمن الدولة – دراسة فقهية مقارنة بالقانون الإماراتي، جمعية دار البر، أبوظبي، ٢٠٢١.

١٠. خالد حسن أحمد لطفى، الأدلة الجنائية الحديثة فى إثبات الجريمة الإلكترونية – دراسة مقارنة، دار الفكر الجامعي، القاهرة ٢٠٢١.

١١. راشد خليفة الغفلي، المواجهة الجنائية للارهاب الالكتروني – دراسة مقارنة، رسالة دكتوراه، كلية الحقوق جامعة عين شمس، القاهرة ٢٠٢١.

١٢. رضا السيد عبد العاطي، الظروف المشددة والمخففة في قانون العقوبات – دراسة فقهية قضائية، دار مصر للنشر والتوزيع، القاهرة ٢٠٢١.

١٣. السيد أحمد محمد علام، جرائم الفساد وآليات مكافحته في نطاق الوظيفة العامة في ضوء التشريع الجنائي المصري والإتفاقيات الدولية – دراسة مقارنة، دار النهضة العربية للنشر والتوزيع، القاهرة ٢٠١٦.

١٤. شريف محسن عبد الفتاح شلتوت، الرقابة على القنوات الإلكترونية – الممارسة والإطار القانوني في ضوء القانون المقارن، دار المعرفة الجامعية، القاهرة ،٢٠٢١.

١٥. ضرغام جابر عطوش آل مواش، جريمة التجسس المعلوماتي – دراسة مقارنة، المركز العربي للنشر والتوزيع، القاهرة، ٢٠١٧.

١٦. عادل أبو القاسم علي عويضة، النظرية العامة للجرائم الماسة بأمن الدولة الداخلي، النهضة العلمية للنشر والتوزيع، القاهرة ٢٠٢٠.

١٧. عبد الحكم سيد سالمان، الجرائم المعلوماتية وأثارها في ضوء قوانين مكافحة جرائم تقنية المعلومات – دراسة مقارنة، مركز الدراسات العربية للنشر والتوزيع، القاهرة ٢٠٢٢.

١٨. عبد الوهاب عبدول، مدخل إلى الجريمة الإرهابية، معهد التدريب والدراسات القضائية، دولة الإمارات العربية المتحدة ٢٠٠٧.

١٩. علي حسن الطوالبة، أبحاث في جرائم تقنية المعلومات – دراسة مقارنة، دار الكتب العربية، عمان ٢٠١٨.

٢٠. غادة نصار، الارهاب والجريمة الالكترونية، دار العربي للنشر والتوزيع، القاهرة ٢٠١٧.

٢١. فاطمة سعيد علي العاصمي، المواجهة الجنائية والأمنية للجرائم الماسة بأمن الدولة الداخلي عبر شبكة الإنترنت، بحث منشور في المجلة القانونية لجامعة القاهرة، المجلد ١٣، العدد ٣، عدد أغسطس ٢٠٢٢.

٢٢. محمد الشبلي العتوم، جرائم تكنولوجيا المعلومات – النظرية العامة للجرائم الإلكترونية – دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان ٢٠٢١.

٢٣. محمد سيد ريان، الشائعات الإلكترونية والأمن السيبراني، دار الجمهورية، القاهرة ٢٠٢٢.

٢٤. محمد علي سويلم، شرح قانون جرائم تقنية المعلومات – القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات – دراسة مقارنة، دار المطبوعات الجامعية، القاهرة ٢٠١٩.

٢٥. محمد علي سويلم، مكافحة الجرائم الإلكترونية – دراسة مقارنة بالتشريعات العربية والأجنبية، دار المطبوعات الجامعية، القاهرة ٢٠٢٠.

٢٦. محمد علي محمد، الإرهاب الإلكتروني بين الفلسفة القانونية وتطور الأمن التقني، دار النهضة العربية للنشر والتوزيع، القاهرة ٢٠١٨.

٢٧. محمود على احمد المردني، النظام القانوني للجريمة الالكترونية المعلوماتية – دراسة مقارنة، دار العلم والإيمان للنشر والتوزيع، القاهرة ٢٠٢٢.

٢٨. نوميد سعيد خضر، دور الصفة الوظيفية فى البنيان القانونى للجريمة، دار الجامعة الجديدة للنشر، القاهرة ٢٠٢٢.

٢٩. هادي محمد ظاهر حسن، الجريمة السياسية وموقع الجرائم منها – دراسة مقارنة، دروب المعرفة للنشر والتوزيع، القاهرة ٢٠٢٢.

٣٠. وسيم الأحمد، مجموعة القوانين العربية المتعلقة بمكافحة جرائم تقنية المعلومات، الدار المنهجية للنشر والتوزيع، عمان، ٢٠٢٠.