جامعة أبوظبي
ABU DHABI UNIVERSITY

كلية القانون College of Law
برنامج الماجستير في القانون العام

الجرائم الإلكترونية الماسة بأمن ومصالح الدولة – دراسة تحليلية

Cybercrime Affecting the Security and Interests of the State - Analytical Study

رسالة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في القانون العام

إعداد الباحث/ سعيد بطي المهيري
الرقم الجامعي: (1075893)

إشراف
الدكتور/ محمد عبد الله العوّا
أستاذ القانون الجنائي المساعد
كلية القانون – جامعة أبوظبي

العام الدراسي 2021-2020

جامعة أبوظبي
ABU DHABI UNIVERSITY

كلية القانون College of Law
برنامج الماجستير في القانون العام

الجرائم الإلكترونية الماسة بأمن ومصالح الدولة – دراسة تحليلية

Cybercrime Affecting the Security and Interests of the State - Analytical Study

رسالة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في القانون العام

إعداد الباحث/ سعيد بطي المهيري
الرقم الجامعي: 1075893

لجنة المناقشة

الدكتور/ حسين عيسى المحمد- أستاذ القانون الجنائي المساعد (رئيسًا)
الدكتور/ محمد عبد الله العوّا - أستاذ القانون الجنائي المساعد (مشرفًا وعضوًا)

العام الدراسي 2021-2020

إقرار الباحث

(أقر أنا الموقع أدناه الطالب/ **سعيد بطي المهيري**. المقيد ببرنامج **(الماجستير في القانون العام)** أن هذا البحث المقدم مني للحصول على درجة الماجستير في القانون العام، هو من نتاج عملي وجهدي العلمي الخالص، وأنه لم يسبق لي التقدم به لأي جهة علمية أو إدارية أو غيرها داخل الدولة أو خارجها للحصول على أي درجة علمية أخرى أو لأي سبب من الأسباب، وأن مضمون هذه الرسالة يعكس آراء الباحث الخاصة وهي ليست بالضرورة الآراء التي تتبناها الجهة المانحة للدرجة العلمية. كما أقر بقبول قيام الجامعة في حال إجازة الرسالة من قِبل لجنة المناقشة والحكم بطباعة الرسالة ونشرها بالكيفية التي تراها محققة لأغراضها وأهدافها، دون أن يكون لي حق العدول عن هذا الإقرار بعد إجازة الرسالة.

اسم الطالب: سعيد بطي المهيري

الرقم الجامعي: 1075893

التوقيع:

جامعة أبوظبي
ABU DHABI UNIVERSITY

إجازة أطروحة الماجستير

عنوان الرسالة:

(" الجرائم الإلكترونية الماسة بأمن ومصالح الدولة – دراسة تحليلية ")

اسم الباحث: سعيد بطي علي المهيري

الرقم الجامعي 1075893

نوقشت هذه الرسالة في يوم **السبت الموافق 2021/4/17 بدءًا من الساعة 12.00 ظهرًا**، وقرر أعضاء لجنة المناقشة المشار إليهم أدناه إجازة الرسالة وهم:

أولًا) **الدكتور/ حسين عيسى المحمد**– أستاذ القانون الجنائي المساعد. (رئيس لجنة المناقشة)

كلية القانون– قسم القانون العام– جامعة أبوظبي.

التاريخ: 17/ 4/ 2021

التوقيع: HOUSAIN ALMOHAMMAD

ثانيًا) **الدكتور/ محمد عبد الله العوّا** – أستاذ القانون الجنائي المساعد. (المشرف والعضو)

كلية– قسم القانون العام – جامعة أبوظبي.

التاريخ: 17/04/2021

التوقيع:

الإهداء

الحمد لله على منه وعونه لإتمام هذا البحث.

إلى من كان لهم الفضل بعد الله والدي العزيزين حفظهما الله ورعاهما.

وإلى أفراد عائلتي وأصدقائي وزملائي الأعزاء.

أهدي هذا الدراسة بكل ود ومحبة ...

الباحث

سعيد بطي المهيري

الشكر والتقدير

أتقدم إلى الله عز وجل بتوفيقه لي لوصولي لهذه المرحلة.

كما أتقدم بالشكر والتقدير والعرفان إلى أصحاب الفضل والمعروف، وأتقدم بالشكر الجزيل والثناء إلى كل من ساعد في إنجاح هذه الرسالة، وأخص بالذكر الاستاذ الدكتور/ محمد عبدالله العوا، المشرف على هذه الرسالة، والذي بذل معي الكثير من الجهد في التوجيه والمتابعة، منذ الخطوات الأولى للبحث، ومنحني المزيد من الوقت لتوجيه النصح والإرشاد، إلى أن ظهر البحث بصورته الحالية.

إلى أساتذتي منذ دراستي لبرنامج البكالوريوس إلى مرحلة الماجستير في القانون العام، والذين لهم الفضل الكبير لوصولي لهذه المرحلة، وإتمام الأطروحة في برنامج الماجستير، أدعوا الله لهم التوفيق والسداد، ولهم التقدير والامتنان.

والشكر موصول لأعضاء لجنة المناقشة الكرام، والذيم كان لملاحظاتهم القيمة أثراً واضحاً في تصويب الرسالة.

الملخص

تناول موضوع الدراسة وصف الجرائم الماسة أمن ومصالح الدولة وفق قانون مكافحة جرائم تقنية المعلومات الاتحادي وتعديلاته، تلك الجرائم التي من شأنها الإضرار بأمن الدولة داخلياً وخارجياً.

ولخطورة هذه الجرائم قام الباحث بالتركيز على الجرائم التي نص عليها القانون بما يخص الجرائم الماسة بأمن الدولة ومصالحها ونصوص التشديد فيها، وقد تناولت الدراسة في المبحث التمهيدي تعريف الجريمة الإلكترونية وركنيها (المادي والمعنوي)، وتوصلت لتعريف الجريمة الإلكترونية الماسة بأمن الدولة: بأنها الجرائم التي تُرتكب عن طريق استخدام أي وسيلة ترتبط بالفضاء الإلكتروني، والغرض منها المساس بأمن الدول ومصالحها، سواءً كان الضرر داخلياً أو امتداده خارجياً.

كما تناولت الركن المادي للجرائم الإلكترونية، وبينت أن المقصود به النشاط أو السلوك المادي في هذه الجرائم، والذي يتطلب وجود بيئة رقمية، واتصال بالشبكة المعلوماتية (الإنترنت)، ويتطلب أيضاً معرفة بداية النشاط والشروع فيه، والنتيجة التي تتحقق منه، كما بينت أن المقصود بالركن المعنوي لهذه الجريمة هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، بتحقق النتيجة بالإرادة والعلم.

وتناول الفصل الأول المواجهة التشريعية للجرائم الإلكترونية الماسة بأمن الدولة، وتم بيان الفرق بين الجرائم الماسة بأمن الدولة الداخلي والخارجي حسب نص القانون في شأن مكافحة جرائم تقنية المعلومات بأركانها المادية والمعنوية، كما تناول أسباب التشديد في هذه الجرائم، والتي بينها الباحث بوصف القانون إلى سبعة جرائم مقسمه على مبحثين.

ثم تناول الفصل الثاني السياسة العقابية لمواجهة الجرائم الإلكترونية الماسة بأمن الدولة ومصالحها، والذي يستوضح الاختصاص القضائي للجرائم الإلكترونية الماسة بأمن الدولة والتدابير العقابية التي نص عليها القانون، وتتكون من ثلاثة أنواع، هي التدابير المقيدة للحرية، والتدابير السالبة للحقوق، والتدابير المادية.

ومن التدابير التي أشار إليها المشرع في قانون مكافحة جرائم تقنية المعلومات المصادرة، وإغلاق المحل أو الموقع الذي أُرتكبت منه الجريمة، والإبعاد، والإشراف والمراقبة والحرمان من استخدام أي شبكة معلوماتية، والإيداع في مأوى علاجي أو مركز تأهيل.

وتوصل الباحث إلى عدة نتائج وتوصيات تم الإشارة إليها، والاستئناس بآراء الفقهاء فيها، وتوضيحها وأخذ ببعضها.

The Summary

The topic of the study and the description of urgent crimes addressed the security and interests of the state in accordance with the Law against It Crimes and its amendments, which would harm the security of the state internally and externally.

The seriousness of these crimes, the researcher focused on the crimes stipulated in the law about crimes against State security and interests and the provisions of emphasis on them. The study addressed a definition of electronic crime in the preliminary research and the pillars of crime with its material, moral integrity and brought it to the definition of cybercrime that is urgent to State security: (crimes committed using any means associated with electronic space and intended to compromise the security and interests of States, whether internally or externally extended).

The physical pillar of cybercrime: physical activity or behaviour in these crimes requires a digital environment and internet connectivity and requires knowledge of the beginning, initiation, and outcome of the activity .

The moral pillar of cybercrime: the psychological state of the offender, and the relationship between the materiality of the crime and the personality of the perpetrator, are intended to achieve the result by will and knowledge.

In the first chapter, he addressed the legislative confrontation of cybercrimes that are urgent to state security, which showed the difference between serious crimes in the internal and external security of the State in accordance with the provision of the law on the fight against IT crimes with their material and moral pillars and addressed the reasons for the emphasis, which the researcher described as seven crimes divided into two .

The second chapter of this study then addressed the punitive policy of dealing with cybercrimes that are urgent to state security and interests, which clarifies the jurisdiction of cybercrimes that are urgent to state security and the punitive measures provided for by law consisting of three types: freedom-restricting measures and negative measures of rights and material measures.

Measures referred to by the legislator in the It Crimes Control Act, such as confiscation, closure of the shop or location where the crime was committed, deportation, supervision, surveillance, denial of the use of any

information network and placement in a treatment shelter or rehabilitation centre.

The researcher reached several results, recommendations that were referred to, based on the opinions of the jurists in them, clarified and took some of them.

المقدمة

الحمد لله رب العالمين القائل في كتابه "وَقُلِ اعْمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ وَسَتُرَدُّونَ إِلَىٰ عَالِمِ الْغَيْبِ وَالشَّهَادَةِ فَيُنَبِّئُكُمْ بِمَا كُنْتُمْ تَعْمَلُونَ" **الآية ﴿١٠٥﴾ سورة التوبة.**

الحمد لله رب العالمين، والصلاة والسلام على رسولنا خير الأنام وخاتم الأنبياء والمرسلين، نحمد الله حمداً كثيراً طيباً أن وفقنا لهذا وهدانا، ونسأله النفع والخير لأمة محمد صلى الله عليه وسلم وللبشرية كافة، أما بعد.

تستمر الحياة في المضي قدماً، وعجلة التقدم والتطور التكنولوجية سائرة بنا لعالم رقمي نعجز عن فهم حيثياته، لشدة تسارع التطور والتقدم فيه، ومع دخول التكنولوجيا والإلكترونيات إلى حياتنا، استجدت الكثير من أنماط الحياة وسبلها، وأصبحت الآلة مهيمنة على حياتنا العلمية والأكاديمية والتربوية بل والاجتماعية منها، حتى أن دخول عالم التكنولوجيا واستخدام الإلكترونيات أصبح من الأمور الحتمية والمقررة علينا، سواءً شئنا أم أبينا، وذلك في المعاملات المصرفية والحكومية والتجارية واللوجستية منها.

وقد عرفنا على مر العصور كيف أن الطرق الإجرامية تتطور في آليتها وطرائقها وفقاً لما هو مستحدث ومعاصر، ومن هنا ظهرت الجرائم الإلكترونية كأساليب احتيالية تستغل ثغرات الحاسب الآلي وثغرات النظم والتطبيقات الإلكترونية، كونه هذه الجرائم تحقق أرباحاً تفوق أرباح الجرائم الواقعية.

وتعتمد هذه الجرائم الإلكترونية على أساليب القرصنة والتزوير والاحتيال والغش من خلال المواقع الإلكترونية وعالم التكنولوجيا المرتبط بالشبكة العنكبوتية (الإنترنت)، والتي منحت المجرمين فرصة كبيرة لتحقيق جرائمهم الإلكترونية من داخل وخارجها، بل ومن أي بقعة في العالم؛ لأن العالم قد أصبح قرية صغيرة بفعل هذا التطور الإلكتروني الهائل.

ولهذا فلابد للقوانين أن تتسم بالمرونة والواقعية، والقابلية للتعديل والحداثة حتى تستطيع الحد من هذه الجرائم الإلكترونية، بالإضافة لسن بعض التشريعات التي تتناسب معها، ولعل هذا ما لفت انتباه الباحث لتكون الجرائم الإلكترونية الماسة بأمن الدولة ومصالحها هي موضوع رسالته، نظراً لأهمية التصدي لهذه الجرائم في حماية أمن الدولة واستقرارها، والمحافظة على مؤشرات النمو والازدهار الاقتصادي بها، وهو ما ينعكس بشكل إيجابي على سعادة وأمن المجتمع بكافة شرائحه.

أهمية موضوع الدراسة:

تظهر أهمية الدراسة في ملامستها لواقعنا المعاصر، فقد زادت معدلات الجرائم الإلكترونية، وتعددت أساليبها، وبالأخص مع توجهات الدول لاعتماد تقنيات الحاسب الآلي والإلكترونيات أساساً لا مجال للاستغناء عنه، بل أصبحت هذه التقنيات مؤشراً من مؤشرات الرخاء والتقدم والتطور، واعتبرت الكثير من الدول التكنولوجيا وتطبيقاتها الإلكترونية الحل الأمثل لمواجهة الظروف الطارئة المتعلقة بالأوبئة، مثل جائحة كورونا (كوفيد 19)، حيث ساهمت هذه التطبيقات التكنولوجية في حماية أرواح الكثير من البشر، وعد توقف نظم العمل والدراسة، وذلك من خلال تيسير شؤون العمل والتعليم لهم من منازلهم.

لذلك كان لابد من حماية مصالح الدولة والعاملين فيها من الجرائم الإلكترونية وانعكاساتها، وخاصة تلك الجرائم التي الماسة بأمن الدولة أسرارها الأمنية، وعدم تعرضها للقرصنة، وكذلك الحفاظ على الودائع المالية، وعدم وقوعها فريسة سهلة للمجرمين.

وقد مثل ذلك حرص الباحث على رفد المكتبة القانونية في دولة الإمارات العربية المتحدة بإحدى الدراسات المتعلقة بهذه الجرائم ومسمياتها، وطرق معالجة القانون لها، ودور المشرع الإماراتي في تحديث وتعديل وسن التشريعات المواكبة لكل الأساليب والطرق الإجرامية الحديثة.

ومن أهمية هذه الدراسة أنها تعكس مدى حرص الباحث على أمن الدولة، وتمثل انعكاساً لصوت المواطنة الصالحة بداخله، لهذا ستتعرض هذه الدراسة لنقاط القوة والقصور في القانون الإماراتي فيما يخص العقوبات، ومدى وكفايته للتصدي لمثل هذه الجرائم، وتتبع القائمين بها، مما ينعكس على مصالح الأفراد داخل وخارج الدولة من مواطنين ومستثمرين ووافدين، ويحقق أمناً إقليمياً ودولياً، وبالتالي تتحقق رؤية الدولة في المضي قدماً نحو الازدهار والتقدم في مجتمع سعيد وأمن تحكمه العدالة، إذ من المهم تمهيد الطريق للأجيال القادمة، بالإضافة لحمايتهم عبر تشريعات واقعية ومنطقية لمكافحة من جميع الجرائم الإلكترونية المستحدثة.

أهداف الرسالة:

تهدف الدراسة من خلال التعرض للجرائم الإلكترونية الماسة بأمن الدولة إلى:

1) التعريف بالجرائم الإلكترونية الماسة بأمن الدولة ومصالحها.
2) استعراض الاختصاص القضائي للجرائم الإلكترونية الماسة بأمن الدولة الداخلي والخارجي منها.
3) التعرف على أوجه الشبه الاختلاف بين الجرائم الماسة بالأمن الداخلي، وبين الجرائم الماسة بالأمن الخارجي من حيث النطاق والعقوبة.
4) اكتشاف السياسة العقابية في التدابير التي وضعها المشرع، وإبعاد الأجنبي والاستثناءات الواردة عليه.
5) استيضاح بعض سياسات التدابير التي نص عليها القانون في الجرائم المرتكبة الماسة بأمن الدولة.

6) تقديم مجموعة من التوصيات والنتائج في ضوء ما ستتوصل إليه دراسة الباحث من نتائج علمية للارتقاء بالبنية القانونية والتشريعية لدولة الإمارات العربية المتحدة.

أسباب اختيار موضوع الدراسة:

1) تفاقم أثر الجرائم الإلكترونية على أمن الأفراد والمجتمعات.

2) مواجهة التطور التكنولوجي الهائل بتشريعات قانونية تأمن انعكاساته السلبية على أمن الدول.

3) شيوع وتعدد الأساليب الإجرامية الإلكترونية في وقتنا هذا.

4) تعتبر دولة الإمارات العربية المتحدة من الدولة ذات معدلات الدخل المرتفع، والتي تستقطب الكثير من المستثمرين مما يجعلها عرضة للإجرام الإلكتروني ومطمعاً له.

5) ارتفاع مؤشرات التطور والتقدم التكنولوجي الهائلة، والتي جعلت دولة الإمارات تستبدل الكثير من المعاملات الورقية بالمعاملات الإلكترونية، وبالتالي ارتفاع معدلات تعرضها للجرائم الإلكترونية.

إشكالية الرسالة:

يُعتبر أمن الدول الحاجة الملحة الأولى والمطلب الأساسي لكل المجتمعات، وبتحققه تتحقق الحياة الكريمة، وتُصان مصالح الأفراد والمجتمعات، ويعم الأمن والأمان، وتزدهر فرص الاستثمار والتطور، وكون الإجرام الإلكتروني يهدد أمن الدولة ومصالحها بنحو عام، ومصالح أفرادها بنحو خاص، فقد كان لابد من اختيار مشكلة تمس هذا المطلب الأساسي (أمن الدولة)، بحيث يمكن حمايته، وتدارك مخاطر المشكلة قبل تفاقمها وتطورها، والتصدي لها بتشريعات مؤهلة ومناسبة وكفيلة بالتصدي لهذه الجرائم الإلكترونية بكافة أشكالها والحد منها، ومن هنا قام الباحث بصياغة إشكالية الدراسة على النحو الآتي:

1) هل تواكب التشريعات والقوانين الإماراتية كافة الجرائم الإلكترونية الحديثة على الساحة الإقليمية والدولية؟

2) هل يُعَاقَب على الجرائم الواقعة خارج إقليم الدولة في قانون مكافحة جرائم تقنية المعلومات؟

3) ما هو الاختصاص القضائي الواجب التطبيق في جرائم أمن الدولة الواقعة خارج الدولة؟ وهل يتم مباشرة الدعوى من خارج الدولة؟ ومن هي السلطة المختصة بتحريك الدعوى؟

4) ما هو نطاق الجرائم الإلكترونية الماسة بأمن الدولة داخلياً أو خارجياً؟

5) ما هي أبرز العقوبات المقررة لمرتكبي الجرائم الإلكترونية الماسة بأمن الدولة؟ وهل العقوبات التي أقرها المشرع الإماراتي في هذا الصدد كافية؟ أم أن هناك بعض القصور الذي يستوجب التغيير؟ وما هو الأساس القانوني في وضع المتهمين في قائمة منع السفر؟

6) هل نص قانون تقنية المعلومات صراحة على حجب المواقع المستخدمة في هذه الجريمة؟ وما هو الأساس القانوني لها؟

7) ما هي فرضية تطبيق تدبير الإبعاد في القانون؟ وهل هناك استثناءات لمرتكب جريمة تمس أمن الدولة للمتهم الأجنبي؟

منهجية الدراسة:

سيستعين الباحث في هذه الدراسة بالمنهج التحليلي الوصفي، وذلك لإضفاء المزيد من الشمولية والموضوعية على موضوع الدراسة، وكذلك لكون هذا المنهج قريباً من الواقع، ويتميز من تمكين الباحث على تحليل الظواهر وجمع المعلومات لتقديم أفضل التوصيات الخاصة بالتشريعات والقوانين، وما يلزم عليها من تعديل أو استحداث.

الدراسات السابقة:

قام بالباحث بالاطلاع على كثير من الدراسات العلمية الخاصة بموضوع الدراسة، واستفاد منها جميعاً في تحديد منهج الدراسة، وفروض البحث، وكثير من المعلومات، ومن تلك الدراسات ما يلي:

الدراسة الأول: دراسة حوراء موسى بعنوان: الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، 2018. قسم المؤلف دراسته إلى الباب الأول في وصفه البناء القانوني للجرائم المرتكبة عبر وسائل التواصل الاجتماعي، وباب آخر الدعوى العمومية الناشئة عن الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، كما تناولت المؤلف جميع مواد قانون مكافحة تقنية جرائم المعلومات لدولة الإمارات، وأيضًا تناول المؤلف تحليل الجرائم الذي نص عليها القانون ذاته، حيث اعتمدت دراستها للسلوكيات المجرمة عبر وسائل التواصل الاجتماعي، كما تناولت دراسة المسؤوليات الجنائية والحالات التي تتوافر فيها المسؤولية الجنائية وإضافة إلى دراسة الإجراءات الجزائية المتبعة في الكشف عن مرتكبي الجرائم الإلكترونية وصولًا للمحاكمة.

الدراسة الثانية: دراسة عبد الرزاق الموافي عبد اللطيف بعنوان: شرح قانون مكافحة تقنية المعلومات، 2016. قسم المؤلف دراسته بكتابين الكتاب الأول تناول فيه إحدى عشر فصل في الجرائم قانون مكافحة جرائم تقنية المعلومات والكتاب الثاني تناول فيه واحد وثلاثون مبحث لباقي الجرائم التي تنص عليها القانون نفسه.

حيث قام الباحث بشرح جميع نصوص مواد قانون مكافحة تقنية المعلومات التي نص عليها القانون، ووصف أركان الجريمة لكل جريمة على حدة، وتناول الكتاب الأول المواد القانونية من المادة (1) إلى المادة (19)، كما أن الكتاب الثاني تناول المواد القانونية من المادة (20) إلى المادة (49).

كما هدف المؤلف إلى توطيد الصلات العلمية والفكرية والإسهام في رفع المستوى العلمي والفقهي في أوساط المجتمع من خلال شرح القانون.

الدراسة الثالثة: دراسة إبراهيم حمد الهنائي وآخرون بعنوان: الجرائم الإلكترونية ودور أجهزة العدالة الجنائية من مواجهتها، 2018. قسم المؤلفين دراسته في سبعة فصول تناول فيها بالفصل الأول تمهيد موضوع البحث، وتناول في الفصل الثاني مفهوم الجريمة الإلكترونية، والفصل الثالث تشريعات مكافحة الجرائم الإلكترونية، والفصل الرابع التحقيق وجمع الأدلة، والفصل الخامس الانتقال بالتحقيق التقليدي إلى التحقيقات الرقمية لمواجهة الجرائم الإلكترونية، والقصل السادس دور أجهزة العدالة في مواجهة الجرائم الإلكترونية، والفصل السابع عرض وتحليل نماذج من قضايا الجرائم الإلكترونية.

كما تناقش الدراسة المتغيرات العلمية والتقنية للجرائم الإلكترونية، وبيات مدلول ومفهوم الجريمة الإلكترونية وجرائم تقنية المعلومات ودراسة دور أجهزة العدالة في مواجهة الجرائم الإلكترونية.

نطاق الدراسة:

تتخصص هذه الدراسة في الجرائم الإلكترونية الماسة بأمن الدولة ومصالحها على وجه العموم، والعقوبات المُشَرَعَة بشأنها على وجه التفصيل والخصوص بدولة الإمارات العربية المتحدة، دون التطرق إلى غيرها من الجرائم الإلكترونية الأخرى التي تقع على الأفراد أو المؤسسات غير الحكومية، أو الجرائم غير الإلكترونية الماسة بأمن الدولة.

المبحث التمهيدي

مفهوم الجرائم الإلكترونية الماسة بأمن الدولة

تُعتبر تقنية المعلومات إحدى نتائج التطور الحضاري والتقدم الذي اجتاح العالم في العصر الحديث، وقد أحدثت تغيراً كبيراً وملموساً كافة مناحي الحياة، ومنها نوعية الجرائم والمجرمين، فبعد أن كانت أغلب الجرائم تعتمد على العنف والقسوة، أصبحت الغلبة الظاهرة تعتمد على القدرات الذهنية والذكاء.[1]

ويشكل موضوع تعريف الجريمة، وتحديد أركانها وبيان أنماطها أهمية خاصة بالنسبة للتدابير الوقائية وخطط مواجهتها، إذ يَصْعُب الحديث عن نشاط اجتماعي سلبي، والدعوة لمواجهته دون تصنيفه من قِبل المجتمع كجريمة يطالها القانون ويحدد لها عقاباً. وفي ضوء تجريم النشاط الاجتماعي السلبي، تتحرك أجهزة العدالة الجنائية نحو مواجهته بكافة تدابير الوقاية والمكافحة، وبين يديها آليات إثبات أركان الجريمة، وإيجاد العلاقة بينها وبين الجاني والضحية.[2]

وتختلف نوعية الجرائم التقليدية عن الجرائم الإلكترونية، فالأولى لها أركانها المادية والمعنوية المعروفة، وظروفها وموقعها وزمانها، بينما الجريمة الإلكترونية هي أقرب ما تكون إلى جريمة تخيلية، حيث تُرتكب هذه الجريمة من خلال الفضاء الإلكتروني، وهو عالم افتراضي متشابك ومتداخل في جميع أنحاء العالم[3]، وفي هذه الدراسة تطرق الباحث لموضوع الجرائم الإلكترونية الماسة بأمن الدولة ومصالحها عبر تقنية المعلومات الإلكترونية، والتعرف على الدور الذي يمارسه قانون دولة الإمارات

---

(1) محمد سالم الزعابي، الجرائم الواقعة على السمعة عبر تقنية المعلومات الإلكترونية، رسالة ماجستير، كلية الشرطة، أبوظبي، 2014، ص 3.

(2) محمد الأمين البشري محجوب، إبراهيم حمد الهنائي، عادل عبدالله حميد، الجرائم الإلكترونية ودور أجهزة العدالة الجنائية من مواجهتها، وزارة الثقافة وتنمية المعرفة، أبوظبي، 2018، ص 22.

(3) حسين بن سعيد الغافري، منظومة سلطنة عمان في التشريعات لمكافحة جرائم تقنية المعلومات، دار النهضة العربية، القاهرة، 2011، ص 15.

العربية المتحدة في التصدي لهذا النوع من الجرائم، والنظر في السلوك الإجرامي في الإثبات الجنائي، والتشديد الوارد في المواد القانونية التي نص عليها القانون.

وانطلاقاً من ذلك قام الباحث بتقسيم المبحث التمهيدي إلى مطلبين، الأول يتناول مفهوم الجريمة الإلكترونية، والثاني يتناول ن الجرائم الإلكترونية الماسة بأمن الدولة، وذلك على النحو التالي:

- **المطلب الأول: ماهية الجرائم الإلكترونية.**
- **المطلب الثاني: أركان الجرائم الإلكترونية الماسة بأمن الدولة.**

المطلب الأول

ماهية الجرائم الإلكترونية

تتوالى على البشرية الثورات المعلوماتية، فما كاد الناس يستفيقون من ثورة المعلومات الجامحة، إلى أن طرأت ثورة جديدة خلقها ذلك التزاوج أو الاتحاد الفريد بين هذا أجهز الحاسب الآلي وأنظمة الاتصالات الحديثة، لنصل في نهاية القرن العشرين وبدايات هذا القرن الواحد والعشرين إلى ما يسمى بالتواصل عبر شبكة الإنترنت، والتي أزاحت الحدود بين الدول، وألغت المسافات بين الأفراد، واختصرت الزمن عبر شبكة لا مرئية أو محسوسة، سميت "بشبكة الإنترنت العالمية"، أو "الشبكة العنكبوتية" أو "الفضاء التخيلي أو السيبراني"(cyberspace).[4]

وقد أشار الباحث (شون ريوردان) [5] في كتابه "الدبلوماسية السيبرانية: إدارة الأمن والحوكمة عبر الإنترنت": إلى أن الفضاء الإلكتروني من ناحية لا يزال فوضوياً، ومن ناحية أخرى يوجد بالفعل تنظيم قابل للإصلاح والتطوير، كما تشير إدارة الإنترنت في العالم بأنه يمكن أن تكون هذه الإدارة تقنية بحتة، ولكنها يمكن أن تتعلق أيضاً بالمسائل المحيطة بحماية البيانات والتشفير، والذي يشكل ليس فقط الإنترنت والفضاء السيبراني، ولكن أيضاً المجتمع الدولي والمحلي، كما ترتكز أيضاً قضايا الحوكمة الرئيسية على استخدام البيانات وحمايتها، بالإضافة لارتباطها بالخصوصية والتشفير، كون الشبكة المعلوماتية قد أنتجت كميات هائلة من البيانات، والتي ترجع أغلبيتها إلى الأفراد حول العام، سواءً من خلال استخدام وسائل التواصل الاجتماعي، أو بطاقات الائتمان، أو تحميل المعلومات الشخصية باستمرار إلى الفضاء الإلكتروني، والكثير من الأفراد يتيحون هذه المعلومات عن غير قصد، نظراً لأن

---

(4) محمد أحمد الحمادي، تشريعات مكافحة جرائم تقنية المعلومات في دولة الإمارات العربية وأحكام القضاء، بحوث ندوة شبكات الإنترنيت وتأثيراتها الاجتماعية والأمنية، القيادة العامة لشرطة أبوظبي، أبوظبي، 2006، ص9.

(5) Cyberdiplomacy, shaun riordan, clays Ltd, London 2019, p. 33.

القليل منهم من يقوم بالاطلاع على شروط وأحكام الخدمات عبر الشبكة المعلوماتية التي يستخدمونها، والتي عادة ما تكون عبارة عن عشرات الصفحات المكتوبة بخط صغير، كما أن الكثير من هؤلاء لا يكون على دراية بالاستخدامات التي يمكن وضع بياناتهم فيها، ومثال على ذلك مواقع التواصل الاجتماعي (Facebook وTwitter وYouTube)، حيث تتيح وسائل التواصل بيانات الأفراد للشركات، لتقوم الشركات بدورها باستخدام هذه البيانات في تسويق منتجاتها.

وتكمن خطورة جرائم الإنترنت والشبكات أو جرائم تقنية المعلومات في كون العالم أصبح يعتمد أكثر فأكثر على الفضاء الإلكتروني (Cyberspace)، لا سيما في البنية التحتية المعلوماتية، سواءً العسكرية أو المصرفية أو الحكومية الاتحادية أو المحلية، إضافة إلى المؤسسات والشركات العامة والخاصة. ولا شك أن زيادة الهجمات الإلكترونية يرتبط أيضاً بازدياد الاعتماد على شبكات الحاسب والشبكة المعلوماتية للبنية التحتية الوطنية الأساسية، وهو ما يعني إمكانية تطور الهجمات الإلكترونية لتصبح سلاحاً حاسماً في النزاعات بين الدول في المستقبل، علماً أن أبعاد مفهوم الحرب الإلكترونية لا يزال غير مفهوم لدى شريحة واسعة من المراقبين، بل وحتى العامة أيضاً.[6]

وقد فرضت التقنيات الإلكترونية والمعلومات نفسها على كثير من المعاملات التي يقوم بها الإنسان خلال ممارسته لحياته اليومية، سواءً بشكل خاص أو عام، مثل استخدام أجهزة الاتصالات الإلكترونية والفضائية، ومروراً بالأعمال الوظيفية، والتراسل بالبريد الإلكتروني، والتجارة الإلكترونية، كما تدخل في وسائل التحكم في الصناعات وأسلحة الدمار الشامل، والتي باتت اليوم رهينة لتقنية المعلومات والاتصالات الإلكترونية.

(6) عمر حامد شكر، المجال الخامس: الفضاء الإلكتروني (دراسات استراتيجية)، المعهد المصري للدراسات، القاهرة، 2019، ص 1.

ولا شك أن هذا التطور والتوسع المتسارع في استخدام التقنيات الإلكترونية للمعلومات والاتصالات على المستويات الوطنية، ومن خلال البنيات التحتية الوطنية للمعلومات، قد ساعد على تزايد فرص الجرائم الإلكترونية وجرائم الفضاء الإلكتروني.[7]

فالجرائم الإلكترونية يصعب حصرها وعدها؛ نظراً لتزايدها، وتنوع أساليبها، وتوسع العالم في استخدام شبكة الإنترنت، فمنها ما يتمثل في استغلال البيانات المخزنة على أجهزة الحاسب الآلية بشكل غير قانوني، ومنها اختراق الحاسب الآلي لتدمير البرامج والبيانات المخزنة عليه، كما تدخل ضمنها الفيروسات الإلكترونية، وعمليات القرصنة الإلكترونية من نسخ برامج أو أفلام أو بيانات أو هجمات تعطيل المواقع، ويمكن القول ببساطة أن الإنترنت ستكون ساحة إجرام مثالية تتحدى الأجهزة الأمنية والقضائية بثغرات قانونية ضخمة، فيمكن حالياً القيام بعملية احتيال على شبكة الإنترنت تُرتكب بين إيطاليا وألمانيا، بينما المنفذون الحقيقيون متواجدون في لندن أو الصين، أو في وسط قرية في شرق آسيا، ويثير هذا الأمر مشكلة قانونية بالاختصاص القضائي والإثبات[8]، وما زالت الأنظمة القانونية وأساتذة القانون في العالم بأسره غير قادرين على الخروج بتصور واضح عن الجريمة الإلكترونية وتفريعاتها الكثيرة المختلفة، وإن كانت الأنظمة القانونية المختلفة تحاول تأسيس أرضية قانونية واضحة للجرائم الإلكترونية.[9]

ولعل الاختلافات في مفهوم أو تعريف الجريمة الإلكترونية يرجع لسرعة تطور التقنية المعلوماتية من جهة، وتباين دور أو شكل الجريمة من جهة أخرى، فالنظام المعلوماتي في هذه التقنية يكون محلاً

(7) محمد الأمين البشري محجوب، الجرائم الإلكترونية ودور أجهزة العدالة الجنائية من مواجهتها، المرجع السابق، ص 22.

(8) بدر الخبيزي، الجرائم الإلكترونية من وجهة نظر اجتماعية، دار دريم بوك، الكويت، الطبعة الثانية، 2017، ص 58.

(9) عماد مجدي عبد الملك، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2011، ص 29.

للجريمة تارة، ويكون وسيلة لارتكابها تارة أخرى، فهناك تعريفات تنطلق من زاوية محل الجريمة بأنها الجريمة المرتكبة بالاعتداء على النظام المعلوماتي، بينما ترتكز تعريفات أخرى على الوسيلة، وكذلك على أشكال السلوك غير المشروع، والذي يرتكز على استخدام الحاسب الآلي.[10]

كما تجدر الإشارة إلى أن أهم العوامل التي أدت لصعوبة الاتفاق على تعريف الجريمة المعلوماتية، هو أن التقنية المعلوماتية أصبحت محل العديد من التقنيات السابقة، كالهاتف والفاكس والتلفاز ، فالمسألة لم تقتصر على معالجة البيانات فحسب، بل تعدتها إلى وظائف عديدة، مثل وظيفة النشر والنسخ، وهو ما يحتم ضرورة التفرقة بين جرائم الإنترنت وشبكات المعلومات بالمعنى الفني، وبين بقية الجرائم الأخرى التي يُستخدم فيها الإنترنت أو الحاسب الآلي كأداة لارتكابها.[11]

ويقصد بجرائم الإنترنت وشبكات المعلومات الدخول غير المشروع إلى الشبكات الخاصة، كالشركات والبنوك وغيرها وكذلك الأفراد، والعبث بالبيانات الرقمية التي تحتويها شبكة المعلومات، مثل تزييف البيانات أو إتلافها أو محوها، وامتلاك أدوات أو كلمات سرية لتسهيل ارتكاب مثل هذه الجرائم التي تلحق ضرراً بالبيانات والمعلومات ذاتها، وكذلك بالنسبة للبرامج والأجهزة التي تحتويها، وهي أيضاً الجرائم التي تلعب فيها التقنية المعلوماتية دوراً رئيسياً في سلوكها الإجرامي.[12]

وهناك من يرى تعريف الجريمة الإلكترونية وفقاً للظاهرة الإجرامية الناشئة عن استخدام تقنية المعلومات، مثال ذلك استخدام الحاسب الآلي في الوصول لمن خدمة الإنترنت وارتكاب أي من الجرائم الواردة ضمن قوانين الدول بحكم سياستها، والتي تُعتبر مخالفة للقانون، مثل جريمة السب، أو الوصول

---

(10) بدر الخبيزي، الجرائم الإلكترونية من وجهة نظر اجتماعية، المرجع السابق، ص 57.

(11) ممدوح خليل عمر، حماية الحياة الخاصة والقانون الجنائي، دار النهضة العربية، القاهرة، 1983، ص 207.

(12) محمد الأمين البشري، المرجع السابق، ص 24.

إلى بيانات بطاقة الدفع الفوري أو الائتمان، أو زرع فيروسات تقوم بتعطيل الأجهزة المركزية، أو اختراق أنظمة الدول، مما يؤدي إلى تدميرها وإتلافها.[13]

ونظراً لعدم استقرار الفقه القانوني على مفهوم محدد للجرائم الإلكترونية أو جرائم تقنية المعلومات بوصفها من الجرائم المستحدثة، والتي لا تزال تحت البحث والدراسة، فقد توصل معظم الباحثين والكتّاب الذين اجتهدوا في دراسة هذا النوع من الجرائم إلى مفاهيم تخدم الباحث من منظور بحثه، باستخدام أساليب ومناهج تلائم المجال الذي تنتمي إليه، لذلك تعددت التعريفات وتفاوتت ضيقاً واتساعاً تبعاً لمعايير دراساتهم، والمنطلقات المستندين إليها.[14]

ويمكن تعريف الجريمة الإلكترونية وفقاً للمعيار الشخصي والموضوعي كالتالي:

المعيار الشخصي:

هي الجريمة أو النشاط غير المشروع الذي يقوم بها الجاني في الدخول إلى المعلومات المخزنة على الحاسب الآلي لحذفها أو تغييرها.

المعيار الموضوعي:

هي الجريمة التي تقوم على إدخال بيانات مزورة في أنظمة الحاسب الآلي، وإساءة استخدامها، إضافة إلى أفعال أخرى تكون أكثر تعقيداً من الناحية إلكترونية.[15]

---

(13) مسعد علي الصباحي الكندي، القانون الواجب التطبيق على الجريمة الإلكترونية، أوراق للنشر والتوزيع، الشارقة، 2019، ص 17.

(14) راشد بشير إبراهيم، التحقيق الجنائي في جرائم تقنية المعلومات: دراسة تطبيقية على إمارة أبوظبي، مركز الإمارات والبحوث الاستراتيجية، أبوظبي، العدد 131، 2008، ص 25.

(15) أمير فرح يوسف، الجريمة الإلكترونية والمعلوماتية وجرائم الإنترنت، مكتبة الوفاء القانونية، الإسكندرية، الطبعة الأولى، 2011، ص 65.

ويرى الباحث أن مفهوم الجرائم الإلكترونية الماسة بأمن الدولة والذي ينصب فيه الموضوع: هي تلك الجرائم التي تُرتكب عن طريق استخدام أي وسيلة ترتبط بالفضاء الإلكتروني، ويكون والغرض منها المساس بأمن الدول ومصالحها، سواءً كان الضرر داخلياً أو كان امتداده خارجياً.

وتستهدف الجرائم التي تُقترف ضد أمن الدولة المساس باستقلال الدولة، أو الانتقاص من سيادتها، وهي تُعتبر من أخطر الجرائم الإلكترونية، خاصة جريمة التجسس والخيانة، أو المساس بأسرار الدولة وإفشائها، أو الجرائم الإرهابية[16]، حيث أتاحت تقنية المعلومات للكثير من الأشخاص المعادين والدول المعادية والمنظمات الإرهابية الترويج لأفكارها ومعتقداتها، بالإضافة إلى أن تقنية المعلومات تعطي فرصاً للتأثير على المعتقدات الدينية وتقاليد المجتمعات، مما يسهل خلق الفوضى داخل الدولة، والمساس بأمنها الداخلي وبنظامها العام.[17]

وقد عالج المشرع الإماراتي في المرسوم بالقانون الاتحادي رقم 05 لسنة 2012 وتعديلاته الخاص بمكافحة جرائم تقنية المعلومات هذه الجرائم، حيث نصت المادة (47) على "مع عدم الإخلال بأحكام الفصل الثاني من الباب الثاني من الكتاب الأول من قانون العقوبات، تسري أحكام هذا المرسوم بقانون على كل من ارتكب إحدى الجرائم الواردة به خارج الدولة، إذا كان محلها نظام معلوماتي إلكتروني أو شبكة معلوماتية أو موقع إلكتروني أو وسيلة تقنية معلومات خاصة بالحكومة الاتحادية، أو إحدى الحكومات المحلية لإمارات الدولة، أو إحدى الهيئات أو المؤسسات العامة المملوكة لأي منهما".

ويُلاحظ أن قانون جرائم تقنية المعلومات الإماراتي قد تميز بقدر كبير من التوسع والشمول، حيث تناول الأفعال والانتهاكات الضارة والخطيرة كافة إذا أُستخدم في ارتكابها الشبكة المعلوماتية أو أي من

---

(16) إبراهيم شاطر محمد الجبوري، جرائم الاعتداء على أمن الدولة من الداخل والخارج، المركز القومي للإصدارات القانونية، القاهرة، الطبعة الأولى، 2011، ص 184.

(17) سامي علي عياد حامد، الجريمة المعلوماتية وإجرام الإنترنيت، دار الفكر الجامعي، الاسكندرية، 2007، ص 77.

وسائل تقنية المعلومات، مما يظهر أن المشرع قد أخذ بمعيار جمع فيه بين الوسيلة المستخدمة وموضوع الجريمة، سواءً أُستخدم فيها جهاز الحاسب الآلي أو أي وسيلة من وسائل تقنية المعلومات، الأمر الذي يعطي القانون قدرة على استيعاب أي أفعال غير مشروعة تُستخدم فيها ابتكارات مستقبلية في مجال تقنية المعلومات.[18]

كما أن التحديد التفصيلي الذي أتى به القانون وشموليته يشير لحرص المشرع على تضمين جميع الانتهاكات في مجال تقنية المعلومات، ووضعها في دائرة التجريم، وخاصة ما ورد من نصوص تتعلق بالأفعال والانتهاكات الماسة بأمن الدولة ومصالحا، سواءً داخلياً أو خارجياً، والذي جاء بلا شك تحت تأثير الانتشار الواسع وغير المقبول لهذا النوع من الانتهاكات التي تُبث عبر الإنترنت ووسائل تقنية المعلومات، والتي أصبحت تشكل خطراً كبيراً على المجتمعات، وبذلك يكون القانون قد عالج واحداً من أهم التحديات التي كانت تواجه أجهزة التحقيق والعدالة الجنائية، بحيث وفر لها الركيزة التشريعية لمواجهة هذا النوع من الجرائم، بأن تم تمييز الأفعال المشروعة من غير المشروعة في مجال استخدامات الحاسب الآلي ونظم تقنية المعلومات.[19]

(18) راشد إبراهيم بشير، التحقيق الجنائي في جرائم تقنية المعلومات، المرجع السابق، ص 45.

(19) راشد إبراهيم بشير، التحقيق الجنائي في جرائم تقنية المعلومات، المرجع السابق، ص 46.

المطلب الثاني

أركان الجرائم الإلكترونية

اختلف الفقه بشأن تحديد الأركان العامة للجريمة، فذهب البعض إلى أن الجريمة لا تقوم إلا على ركنين، هما الركن المادي والركن المعنوي، بينما ذهب آخرون إلى أن للجريمة ثلاثة أركان، هي الركن الشرعي والركن المادي والركن المعنوي.

وذهب الفقه التقليدي إلى أن الجريمة تقوم على ركنين لا ثالث لهما، هما الركن المادي والركن المعنوي، الركن الأول يُعبر عنه بالسلوك المادي الذي أخل بالمصلحة التي يحميها المشرع، سواءً أكان هذا السلوك إيجابياً أم سلبياً، ويدخل في إطار هذا السلوك النتائج التي تحيط به، ويأخذها المشرع بعين الاعتبار، أما الركن الثاني فيُعبر عنه بالقوة النفسية التي تسيطر على السلوك المادي، وتربط بينه وبين النتيجة المترتبة عليه، فالجريمة ليست محض سلوك ضار أو خطر، ولكنها في الوقت ذاته وبالنسبة لمن يقترفها انحراف عن الواجب يستحق اللوم والمؤاخذة، وهذا جوهر الركن المعنوي، ويذهب هذا الاتجاه إلى أن تقييم المشرع للجريمة بركنيها، وإضفاء الصفة غير المشروعة عليها، لتعارضها مع أوامره ونواهيه، لا يدخل في عداد أركان الجريمة، وإنما تُعبر هذه الصفة عن جوهر الجريمة ذاتها[20]؛ ولذلك فإن الجريمة تكون ذات ركنين فقط، هما الركن المادي والركن المعنوي.

بينما ذهب الفقه الجنائي الحديث إلى أن للجريمة ثلاثة أركان، هي الركن الشرعي والركن المادي والركن المعنوي، ويتحقق الركن الشرعي عندما يتطابق السلوك المادي المُقْتَرَف من الجاني مع نص

(20) علي محمود علي حمودة، قانون العقوبات: النظرية العامة للجريمة، أكاديمية شرطة دبي، دبي، الطبعة الثانية، 2008، ص 117.

من نصوص التجريم والعقاب، شريطة ألا يكون هذا خاضعاً لسبب من أسباب الإباحة، فيقوم هذا الركن بمخالفة الواقعة المادية للغاية التي تهدف إلى تحقيقها.[21]

ولا تقوم أي جريمة ولا تتم المعاقبة عليها إلا إذا استوفت جميع أركانها الأساسية التي تُبنى عليها، وذلك وفقاً للمبدأ المتعارف عليه بأن لا جريمة ولا عقوبة إلا بنص، فلا تقوم أو تنشأ المسؤولية الجنائية إلا إذا توافرت جميع أركان الجريمة، وفي حال تعذر أي ركن من أركانها، فلا يُعد الفعل جريمة، ولا تقام المسؤولية الجنائية على مرتكبه.[22]

والأصل أن لكل جريمة ركنيها المادي المعنوي، وإذ تخلف أحدهما أُعتبر الفعل غير مجرم، كما تطلب القانون لبعض الجرائم قصداً خاصاً، ويُقصد بالركن المادي للجريمة كما جاء في المادة (31) من قانون العقوبات الاتحادي وتعديلاته "أي نشاط إجرامي بارتكاب فعل أو الامتناع عن فعل متى كان هذا الارتكاب أو الامتناع مجرم قانوناً.[23]

أما الركن المعنوي للجريمة فيُقصد به العمد أو الخطأ وفقاً للمادة (38) من قانون العقوبات الاتحادي، والتي نصت على "ويتوفر العمد باتجاه إرادة الجاني إلى ارتكاب فعل أو الامتناع عن فعل متى كان هذا الارتكاب أو الامتناع مجرماً قانوناً وذلك بقصد إحداث نتيجة مباشرة أو أية نتيجة أخرى مجرمة قانونا يكون الجاني قد توقعها".[24]

---

(21) علي محمود علي حمودة، قانون العقوبات: النظرية العامة للجريمة، المرجع السابق، ص 118.

(22) خالد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت: دار الثقافة، عمّان، الطبعة الأولى، 2011، ص 31.

(23) المادة (31) من المرسوم بقانون اتحادي رقم (7) لسنة 2016م بتعديل بعض أحكام قانون العقوبات الصادر بالقانون الاتحادي رقم (3) لسنة 1987م.

(24) المادة (38) من المرسوم بقانون اتحادي رقم (7) لسنة 2016م بتعديل بعض أحكام قانون العقوبات الصادر بالقانون الاتحادي رقم (3) لسنة 1987م.

أما الخطأ فيتوفر بوقوع النتيجة الإجرامية بسبب خطأ الفاعل، سواءً بإهماله أو عدم انتباهه أو عدم احتياطه، أو طيشاً أو رعونة، أو عدم مراعاة للقوانين واللوائح والأنظمة، إذاً فأركان الجريمة الإلكترونية كما ذُكر آنفاً هي تلك التي تتم باستخدام حاسب آلي أو وسيلة إلكترونية، أو من خلال وسيلة تقنية المعلومات، وقد تتشابه الجريمة الإلكترونية والجريمة التقليدية في بعض الأمور، ولكنها تختلف عنها أيضاً في كثير من الأمور.[25]

(25) طارق أحمد فتحي سرور، الحماية الجنائية لأسرار الأفراد في مواجهة النشر، دار النهضة العربية، القاهرة، 2001، ص 51.

الفرع الأول

الركن المادي في الجرائم الإلكترونية

إن النشاط أو السلوك المادي في الجرائم الإلكترونية يتطلب وجود بيئة رقمية، واتصال بالشبكة المعلوماتية، ويفرض أيضاً معرفة ببداية هذا النشاط والشروع فيه، ونتيجته التي تترتب عليه، فمثلاً يقوم مرتكب الجريمة بتجهيز الحاسب أو الجهاز الإلكتروني لكي يحقق له حدوث الجريمة، فيقوم بتحميل الجهاز الإلكتروني أو الحاسب الآلي ببرامج اختراق، أو بقيامه بإعدادها بنفسه، وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد داعرة أو مخلة بالآداب العامة، وتحميلها على الجهاز المضيف Hosting Server، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيداً لبثها.[26]

ولا تستلزم كل جريمة وجود أعمال تحضيرية، وفي الحقيقة يصعب الفصل بين العمل التحضيري، وبداية النشاط الإجرامي في جرائم الحاسب الآلي والشبكة المعلوماتية، حتى ولو كان القانون لا يعاقب على الأعمال التحضيرية، إلا أنه في مجال تكنولوجيا المعلومات يختلف الأمر بعض الشيء، فشراء برامج اختراق، ومعدات لفك الشفرات وكلمات المرور، وحيازة صور دعارة للأطفال، فمثل هذه الأشياء تمثل جريمة في حد ذاتها.[27]

وتثير مسألة النتيجة الإجرامية في جرائم الإنترنت مشاكل عدة، ومنها على سبيل المثال مكان وزمان تحقق النتيجة الإجرامية، ومثال عليه قيام أحد الجناة بارتكاب جريمة عن طريق استخدام الحاسب الآلي، وتثبيت برامج اختراق، أو قيامه بإعدادها بنفسه، أو إعداد برامج فيروسات تمهيداً لبثها، كما لا يستلزم لكل جريمة وجود أعمال تحضيرية.

---

(26) لينا جمال محمد، الجرائم الإلكترونية، دار خالد الليحاني، عمّان، 2016، ص 91.

(27) لينا جمال محمد، الجرائم الإلكترونية، المرجع السابق، ص 91.

وفي الحقيقة يصعب الفصل بين العمل التحضيري، وبداية النشاط الإجرامي في الجرائم الإلكترونية، حتى ولو كان القانون لا يعاقب على الأعمال التحضيرية، إلا أن الأمر يختلف في مجال تكنولوجيا المعلومات، فشراء برامج اختراق وبرامج فك شفرات وكلمات المرور، تمثل هذه المشتريات جريمة في حد ذاتها، وتأتي مسألة النتيجة الإجرامية في الجرائم الإلكترونية بعدة تعقيدات، فعلى سبيل المثال تتحقق النتيجة الإجرامية بالمكان والزمان، فلو قام أحد المجرمين في أمريكا اللاتينية باختراق جهاز خادم (Server) أحد المصارف في الإمارات، وكان هذا الخادم موجوداً في الصين، فكيف يمكن معرفة وقت حدوث الجريمة؟ هل هو توقيت بلد المجرم؟ أم توقيت بلد البنك المسروق؟ أم توقيت الجهاز الخادم في الصين؟ ويثار هنا أيضاً إشكاليات القانون الواجب التطبيق في هذا الشأن، حيث إن هناك بعداً دولياً في هذا المجال.[28]

(28) بدر الخبيزي، الجرائم الإلكترونية من وجهة نظر اجتماعية، م المرجع السابق، ص 72.

الفرع الثاني

الركن المعنوي في الجرائم الإلكترونية

يقصد بهذا الركن الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، فالقصد الجنائي في جريمة الدخول غير المصرح به هي نية الجاني في الولوج إلى حاسب آلي مثلاً، ثم يَلْزَم إثبات نية الجاني في تحدي الحظر الوارد على استخدام المعلومات بتحقيق النتيجة بالإرادة والعلم.[29]

وقد برزت تلك المشكلة في القضية المعروفة بقضية موريس، والذي كان الجاني فيها متهماً بدخول غير مصرح به على جهاز حاسب آلي فيدرالي، وقد دفع محامي موريس بانتفاء الركن المعنوي، الأمر الذي جعل المحكمة تقول: «هل يلزم أن يقوم الادعاء بإثبات القصد الجنائي في جريمة الدخول غير المصرح به، بحيث تثبت نية المتهم في الولوج إلى حاسب فيدرالي، ثم يَلْزَم إثبات نية المتهم في تحدي الحظر الوارد على استخدام نظم المعلومات في الحاسب وتحقيق خسائر، ومثل هذا الأمر يستدعي التوصل إلى تحديد أركان جريمة الدخول دون تصريح.[30]

إلا أن بعض القوانين مثل القانون الفرنسي جاء فيها الركن المعنوي من منطلق أن سوء النية هو الأعم شأن الجرائم الإلكترونية، حيث اشترط المشرع الفرنسي وجود سوء نية الاعتداء مثلاً على البريد الإلكتروني الخاص بأحد الأشخاص، هذا ويمكن القول أيضاً بتوافر الركن المعنوي في الجرائم الإلكترونية أو جرائم الإنترنت في المثال الخاص بقيام أحد القراصنة بنسخ برامج حاسب آلي من موقع على شبكة

(29) علاء الدين منصور، الأوجه الحديثة للجرائم المعلوماتية، جامعة الحكمة، بيروت، 2000، ص 18.
(30) لينا جمال محمد، الجرائم الإلكترونية، المرجع السابق، ص 92.

المعلومات، والقيام بفك شفرة الموقع وتخريبه للحصول على البرمجيات، من أجل الضرر بالمجني عليه سواءً كان شخصاً طبيعياً أو معنوياً.

ويمكن القول أيضاً بتوافر الركن المعنوي في جرائم الإنترنت في حال قيام أحد القراصنة بنسخ برامج حاسب من موقع على شبكة الإنترنت، والقيام بفك شفرة الموقع وتخريبه للحصول على البرمجيات وإيقاع الأذى بالشركة.

ويرى الباحث من خلال ما تم توضيحه من مقصد الركنين المادي المعنوي للجريمة الواقعة على الشبكة المعلوماتية، باستخدام تقنية المعلومات من خلال سوء استخدام الأنظمة أو الشبكات الإلكترونية بطريقة غير مشروعة، أو اقتحام آثار مادية ملموسة تساهم في تدمير المعلومات، أو التزوير والتلاعب في البيانات المرتبطة بالحاسبات الآلية، وتخلف كل جريمة من جرائم تقنية المعلومات بأركانها المادية والمعنوية، والتي سيتم التفصيل فيها خلال الفصل الأول لكل جريمة ماسة بأمن الدولة على حدة، لكونها تدخل في صلب موضوع الدراسة.

والوصول إلى المجرم المعلوماتي أو الإلكتروني لإيقاع المسئولية الجنائية عليه يشكل عبئاً فنياً وتقنياً بالغاً على القائمين بأعمال التتبع والتحليل لملابسات الوقائع الإجرامية المختلفة، وقد نصت المادة (12) من معاهدة بودابست لمكافحة جرائم الفضاء المعلوماتي – والتي لم تكن الولايات المتحدة طرفاً فيها، وسارعت بالانضمام إليها بعد أحداث الحادي عشر من سبتمبر 2001 – على "سوف يتبنى كل طرف تدابير تشريعية، وأي تدابير أخرى لضمان قيام مسؤولية الأشخاص المعنوية عن أي جريمة موصوفة في هذه المعاهدة، إذا ما أُرتكبت لصالح الشخص المعنوي بواسطة شخص طبيعي اقترفها بشكل منفرد، أو بوصفه جزءاً من عضو في الشخص المعنوي على أساس من:

- تفويض من الشخص المعنوي.
- سلطة اتخاذ قرارات لصالح الشخص المعنوي.

- سلطة لممارسة رقابة أو سيطرة داخل الشخص المعنوي.

إلى جانب الحالات الواردة في البند (1) سوف يتخذ كل طرف التدابير اللازمة لضمان قيام مسؤولية الشخص المعنوي، إذا ما أدي نقص الإشراف أو السيطرة من قبل الشخص الطبيعي المشار إليه في الفقرة (1) إلى إمكانية ارتكاب جريمة قائمة طبقاً لهذه المعاهدة لصالح الشخص المعنوي بواسطة شخص طبيعي اقترفها تحت سيطرته".[31]

(31) لينا جمال محمد، الجرائم الإلكترونية، المرجع السابق، ص 94.

الفصل الأول

المواجهة التشريعية للجرائم الإلكترونية الماسة بأمن الدولة

يُقصد بالجرائم الماسة بأمن الدولة تلك الجرائم التي تضر بسلامة الدولة، سواءً كانت تلك التي تمس أمن الدولة داخلياً أو خارجياً، وتُصنف هذه الجرائم من أخطر الجرائم التي تهدد كيان الدولة، حيث يهدف مقترفوها لهدر القيم الأدبية والمادية للدولة.

ومن الواضح أن أول الجرائم التي ظهرت في تاريخ التشريعات الجنائية كانت جرائم موجهة ضد المصالح العامة للجماعات، وكان يُعَاقَب عليها بعقوبة مشددة، حيث عاقبت التشريعات الجنائية الوضعية والعرفية على الجرائم التي ترتكب ضد المجموع بعقوبات يغلب عليها طابع القسوة الواضحة، بينما الجرائم المرتكبة ضد الأفراد كانت خلافاً لذلك، فهي تُعد جرائم مألوفة بين المجرم والمعتدى عليه.

ولأن القضايا التي تتسم بالخطورة كانت تلحق ضرراً بالمصالح العامة، فكانت تصل عقوبتها إلى الإعدام أو النفي، حيث كانت التشريعات تهتم بوضع قواعد وأسس واضحة للتصدي لجميع الجرائم الماسة بأمن الدولة في جميع مجالاته، ومواجهتها بفرض عقوبات مشددة على مرتكبها.

وقد ظلت العقوبات حتى الوقت الحالي بصفتها الشديدة ذاتها تجاه من يرتكب جريمة ماسة بأمن الدولة، فمهما بلغت الدول من درجات التحضر والرقي في التعامل مع المجرمين، وفي سياستها العقابية، إلا أن كل دولة تحاول جاهدة الحفاظ على أمنها، وعلى سلامة حدودها، وتقوية تماسكها، وعدم التسامح مع مواطنيها الذين يقيمون علاقات أو صلات مع الجماعات المعادية لها.[32]

وقد أدى التطور الإلكتروني والمعلوماتي، وتعاملات الدول عبر الشبكات الإلكترونية من خلال تخرين البيانات، والتراسل فيما بين الدول لفرض قوانين أخرى في مجال تقنية المعلومات للتصدي لجرائم

(32) إبراهيم شاطر محمد الجبوري، جرائم الاعتداء على أمن الدولة من الداخل والخارج، المرجع السابق، ص 13.

تقنية المعلومات، خاصة أنه كثيراً ما تكون الدوافع وراء ارتكابها دوافع سياسية، تهدف لتهديد الأمن القومي والعسكري، حتى أصبح ما يُعرف الآن بحرب المعلومات، والتجسس الإلكتروني، والإرهاب الإلكتروني.[33]

وقد نصت المادة (44) من المرسوم بقانون 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات على "تُعتبر الجرائم الواردة في المواد (4، 24، 26، 28، 29، 30، 38) من هذا المرسوم بقانون من الجرائم الماسة بأمن الدولة، كما تُعتبر من الجرائم الماسة بأمن الدولة، أي جريمة منصوص عليها في هذا المرسوم بقانون إذا ارتكبت لحساب أو مصلحة دولة أجنبية أو جماعة إرهابية أو مجموعة أو جمعية أو منظمة أو هيئة عير مشروعة".

لذلك تم تقسيم هذا الفصل لمبحثين، تناول الأول الجرائم الإلكترونية الماسة بأمن الدولة من الداخل، تناول الثاني الجرائم الإلكترونية الماسة بأمن الدولة من الخارج، وذلك على النحو التالي:

- **المبحث الأول: الجرائم الإلكترونية الماسة بالأمن الداخلي.**
- **المبحث الثاني: الجرائم الإلكترونية الماسة بالأمن الخارجي.**

(33) حسين بن سعيد الغافري، منظومة سلطنة عمان في التشريعات لمكافحة جرائم تقنية المعلومات، المرجع السابق، ص 13.

المبحث الأول

الجرائم الإلكترونية الماسة بالأمن الداخلي

سيتم تقسيم هذا المبحث لمطلبين، يتناول الأول نطاق تطبيق القانون على الجرائم الماسة بأمن الدولة ومصالحها الداخلية، وموقف المشرع الإماراتي منها، بينما يتناول المطلب الثاني أنواع الجرائم من حيث أركان الجريمة والتشديد وفقاً لما نص عليه المرسوم بقانون رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، وذلك على النحو التالي:

- **المطلب الأول: نطاق جرائم أمن الدولة الداخلي.**
- **المطلب الثاني: أنواع الجرائم الإلكترونية الماسة بأمن الدولة الداخلي.**

المطلب الأول

نطاق جرائم أمن الدولة الداخلي

يُقصد بأمن الدولة من الداخل سيادة الحكومة على المحكومين، سواءً من الناحية المادية بكونها قابضة على زمامهم، أو من الناحية المعنوية بكونهم يبدون لها الطاعة والولاء، وهذا الأمر هو الذي تتمثل فيه الجرائم المضرة بأمن الدولة.

ويُعتبر قانون العقوبات من أكثر القوانين التصاقاً بسيادة الدولة، فهو يطبق بسلطتها، ولأجل توفير الحماية لها ولكافة الأفراد الذين يعيشون على الإقليم الذي يخضع لسيادتها؛ ولذلك فإن الدولة هي التي تملك سلطة العقاب على كل من ينتهك نصوص التجريم والعقاب في كافة عناصر إقليمها.

وبالنظر إلى ارتباط التجريم والعقاب بسيادة الدولة، فقد جعل نطاق تطبيق نصوص التجريم والعقاب النافذة على الجرائم المرتكبة في النطاق المكاني لكافة عناصر الإقليم الخاضع لسيادة الدولة ويسمى بالشق الإيجابي، وشق آخر يدعى بالشق السلبي وهو عدم امتداد قانون العقوبات لملاحقة الجرائم التي ترتكب خارج الإقليم الخاضع لسيادة الدولة.

وإذا كان تطبيق قانون العقوبات من حيث المكان يدور في فلك هذين الشقين، إلا أن هناك اعتبارات معينة قد أدت إلى الخروج عليهما، فقد أصبح في الإمكان سريان القانون الوطني على جرائم ترتكب خارج إقليم الدولة لحماية مصلحتها، وأصبح في الإمكان كذلك عدم تطبيق القانون الوطني على بعض الجناة الذين يرتكبون جرائمهم على الإقليم الوطني؛ بسبب عدم خضوعهم للقضاء الوطني لاعتبارات قد تكون داخلية أو دولية.

وقد نص قانون العقوبات الاتحادي على مبدأ الإقليمية في المادة (16)، حيث نصت على "تسري أحكام هذا القانون على كل من يرتكب جريمة في إقليم الدولة"، كما نص المشرع المصري نص عليه

أيضاً في قانون العقوبات، فقد نصت المادة (1) على "تسري أحكام هذا القانون على كل من يرتكب في القطر المصري جريمة من الجرائم المنصوص عليها فيه"[34].

ويتم تطبيق المادة (16) المتقدم ذكرها بقانون العقوبات الاتحادي على جميع الجرائم التي ترتكب داخل النطاق الإقليمي الخاضع لسيادة دولة الإمارات العربية المتحدة، دون الاعتداد في ذلك بجنسية مرتكب الجريمة.

ولعل تطبيق قانون العقوبات الاتحادي الوطني على كافة الجرائم التي تقع في النطاق المكاني الخاضع لسيادة دولة الإمارات العربية المتحدة يستند لمضمون مبدأ الإقليمية ذاته، ويستند كذلك إلى المبررات التي جعلت كافة الدول تأخذ بهذا المبدأ، وتحرص على النص عليه في تشريعاتها الوطنية، كذلك فإن التطبيق الصحيح لمبدأ الإقليمية يتطلب تحديد الضابط الذي يطبق في إطاره[35].

وفي إطار قانون جرائم تقنية المعلومات، فالجرائم المضرة بأمن الدولة من الداخل هي تلك الجرائم التي تنطوي على الاعتداء على النظام الداخلي للدولة، والمساس بالأمن والاستقرار الذي يتمتع به الناس، سواءً كان المساس بالنظام الاجتماعي أو السياسي أو الاقتصادي أو بنظام الحكم، وتجريم الاعتداء على أمن الدولة من الداخل يهدف لحماية أمن الناس واستقرارهم، فالحفاظ على استقلال الدولة وسيادتها هي محل الحماية في تجريم الاعتداء على أمن الدولة من الخارج[36].

وقد قام المشرع الإماراتي بالنص على جرائم أمن الدولة الداخلية في عدة تشريعات، تناول فيها أهم الجرائم الماسة بأمن الدولة الداخلي، ويُعد قانون العقوبات الاتحادي رقم 3 لسنة 1987 وتعديلاته هو

(34) المادة (1) من قانون العقوبات المصري رقم 58 لسنة 1937 وفقاً لآخر بالقانون رقم 189 لسنة 2020.

(35) علي محمود علي حمودة، قانون العقوبات: النظرية العامة للجريمة، المرجع السابق، ص 73.

(36) أحمد فتحي سرور، الوسيط في قانون العقوبات، دار النهضة العربية، القاهرة، الطبعة السادسة، 2015، ص 45.

التشريع الأول في حماية المجتمع من هذه الجرائم، وردع مرتكبيها، حيث كان هذا التشريع هو الأول الذي يتناول هذه الجرائم، ويقرر مواجهتها بعقوبات رادعة.[37]

كما قنن المشرع في قانون العقوبات الاتحادي هذه الأحكام، فتنص المادة (16) على "تسري أحكام هذا القانون على كل من يرتكب جريمة في إقليم الدولة، ويشمل إقليم الدولة أراضيها، وكل مكان يخضع لسيادتها بما في ذلك المياه الإقليمية والفضاء الجوي الذي يعلوها، وتُعتبر الجريمة مرتكبة في إقليم الدولة إذا وقع فيها فعل من الأفعال المكونة لها، أو إذا تحققت فيها نتيجتها، أو كان يراد أن تتحقق فيها".[38]

وعلى ضوء مبدأ الإقليمية، فإن تطبيقه يحتاج إلى ضابط معين عن طريقه يمكن تحديد الإقليم الذي يُطبق فيه قانون العقوبات الوطني لتطبيق قانون تقنية المعلومات، وعن طريقه يمكن أيضاً تحديد الزمن الذي تُعتبر الجريمة قد وقعت في نطاق هذا الإقليم؛ وذلك لكي يُطَبَق عليها هذا القانون، وبنص المادة (16) من قانون العقوبات الاتحادي سالف الإشارة إليها على بيان المقصود بالإقليم، فقد ذكرت بأن الإقليم يشمل أراضي الدولة، وكل مكان يخضع لسيادتها بما في ذلك المياه الإقليمية، والفضاء الجوي الذي يعلوها، كذلك فإن هناك حالات يمتد فيها الإقليم بنصوص قانونية، ويترتب عليها تطبيق القانون الوطني، وهو ما يحدث بشأن السفن والطائرات[39].

وتطبيق قانون العقوبات من حيث المكان من خلال إقليم الدولة هو عبارة عن مساحة اليابس التي تنحصر نطاق الحدود السياسية للدولة، ويشمل هذا الإقليم ما تحت هذا اليابس من طبقات الأرض، كما يتضمن هذا الإقليم مساحة الماء التي تقع داخل الحدود السياسية للدولة، وكذلك بحرها الإقليمي،

---

(37) أحمد غانم سيف السويدي، المواجهة الجنائية والأمنية للجرائم الماسة بأمن الدولة الداخلي، رسالة ماجستير، أكاديمية شرطة دبي، دبي، 2015، ص 14.

(38) علي محمود علي حمودة، مرجع السابق، ص 74.

(39)علي محمود علي حمودة، ص 75.

ويتضمن المياه الداخلية للدولة (الأنهار الوطنية، والأجزاء التابعة للدولة من الأنهار الدولية، والبحيرات، والبحار المغلقة، والقنوات، والمضايق والخلجان، والموانئ البحرية)، وأما البحر الإقليمي فهو عبارة عن الجزء من البحر العام الملاصق لشواطئ الدولة، والذي أصبح يتم تحديده وفقاً للعرف الدولي، وأيضاً وفقا لأحكام الاتفاقية الدولية الصادرة سنة 1985 بشأن البحر الإقليمي، والتي نصت على أن مساحته لا تتجاوز اثنى عشر ميلاً بحرياً (المادة 24 من هذه الاتفاقية).

كما يشمل هذا الإقليم طبقات الهواء التي تعلو الإقليم الأرضي للدولة، وأيضاً إقليمها الجوي، وإلى ما لا نهاية في الارتفاع، وأما طبقات الجو العليا والأجرام السماوية فلا تخضع لسيادة أي دولة، فهي بمثابة الفضاء الحر، وذلك وفقاً لأحكام الاتفاقية الخاصة بتنظيم استغلال الدولة للطبقات العليا في الجو، والتي وافقت الجمعية العامة للأمم المتحدة على مشروعها في 19 ديسمبر 1961م، ويُسمى بالإقليم الجوي[40].

وتحرص الكثير من الدول على النص في تشريعاتها على خضوع الجرائم التي تقع على السفن التي تحمل علمها لقانونها الوطني، وكذلك على الطائرات التي تحمل جنسيتها، وتنظم المادتان (١٧، ١٨) من قانون العقوبات الاتحادي تطبيق هذا القانون بالنسبة للجرائم التي ترتكب على ظهر السفن والطائرات التي تحمل علم دولة الإمارات العربية المتحدة، وبموجب هاتين المادتين يمكن تحديد القانون الواجب التطبيق على الجرائم التي تقع على ظهر السفن والطائرات على النحو الآتي:

أ- وفقاً لنص المادة (١٧) سالف الإشارة إليها، فإن كافة الجرائم التي ترتكب على ظهر السفن والطائرات التي تحمل علم دولة الإمارات العربية المتحدة، أو تحمل جنسيتها، سواءً أكانت

(40) عبد العظيم مرسي وزير، شرح قانون العقوبات: القسم العام، الجزء الأول، دار النهضة العربية، القاهرة، الطبعة الرابعة، 2006، ص 80.

حربية، أم كانت تملكها الدولة وتديرها لأغراض غير تجارية، فإنها تخضع لقانون العقوبات الوطني أينما وجدت.

ب- وفقاً لنص المادة (١٨) سالف الإشارة إليها، فإن كافة الجرائم التي ترتكب على ظهر السفن والطائرات الأجنبية في أحد موانئ دولة الإمارات العربية المتحدة أو في بحرها الإقليمي، تخضع – كقاعدة عامة – لقوانين الدول التي تحمل أعلامها، أو تحمل جنسيتها.

لكن المشرع الإماراتي أورد على هذه القاعدة حالات استثنائية، إذا توافرت فإنه يترتب عليها تطبيق قانون العقوبات الاتحادي الوطني، وفرق المشرع في هذه الحالات بين السفن والطائرات على النحو الآتي:

أ- بالنسبة للسفن:

1) إذا امتدت آثار الجريمة إلى الدولة.
2) إذا كانت الجريمة بطبيعتها تمس أمن الدولة، أو تعكر السلم فيها، أو تخل بالآداب العامة، أو حسن النظام في موانيها، أو بحرها الإقليمي.
3) إذا طلب ربان السفينة أو قنصل الدولة التي تحمل علمها المعونة من السلطات المحلية.
4) إذا كان الجاني أو المجني عليه من مواطني الدولة.
5) إذا كانت السفينة تحمل مواد أو أشياء محظور تداولها أو حيازتها أو الاتجار فيها دولياً.

ب-بالنسبة للطائرات:

1) إذا حطت الطائرة في إحدى مطارات دولة الإمارات العربية المتحدة بعد ارتكاب الجريمة.
2) إذا كانت الجريمة بطبيعتها تعكر السلم في الدولة، أو تخل بنظامها العام.
3) إذا شكلت الجريمة مخالفة للوائح والأحكام المنظمة لحركة الملاحة الجوية في الدولة.
4) إذا طلب قائد الطائرة المعونة من السلطات المحلية.

5) إذا كان الجاني أو المجني عليه في الجريمة التي وقعت على ظهر الطائرة من مواطني الدولة.

وإذا كان يلزم لتطبيق قانون العقوبات الاتحادي وقوع الجريمة في النطاق المكاني لعناصر الإقليم على النحو سالف الإشارة إليه، إلا أن ذلك لا يكفي لكي يُطَبَق هذا القانون تطبيقاً سليماً، وإنما الأمر يحتاج إلى تحديد مكان وقوع الجريمة؛ وذلك لإمكان القول بأنها قد وقعت في النطاق المكاني السابق تحديده.

كما تناول المشرع الإماراتي الجرائم الماسة بأمن الدولة الداخلي في قانون مكافحة جرائم تقنية المعلومات رقم 5 لسنة 2012 في المواد (4، 20، 28، 29، 30)، وقد تضمنت الجرائم الماسة بأمن الدولة وصورها.

وتُعد أخطر الأفعال غير المشروعة التي جَرّمها المشرع الإماراتي لحماية أمن الدولة الداخلي هي جرائم الدخول بدون تصريح، بقصد الحصول على بيانات حكومية، وجرائم إثارة الفتنة أو الكراهية أو العنصرية، أو الإضرار بالوحدة الوطنية أو السلم الاجتماعي، وجرائم تعريض أمن الدولة ومصالحها للخطر، والمساس بالنظام العام، والجرائم المتعلقة بالسخرية أو الإضرار بسمعة وهيبة ومكانة الدولة أو أي من مؤسساتها، أو رئيسها وحكامها أو أولياء عهودها، أو علمها أو سلامها الوطني أو رموزها، والجرائم المتعلقة بقلب نظام الحكم في الدولة أو الاستيلاء عليه، أو تعطيل أحكام الدستور أو القوانين السارية في البلاد.

أمثلة قضائية على نطاق الإقليم:

في حكم محكمة تمييز رأس الخيمة، قضت محكمة الجنايات حضورياً بجلسة 13 من ديسمبر سنة 2006م بمعاقبة المتهم بالحبس والغرامة بناء على التهم الموجهة له، فقام المحكوم عليه باستئناف الحكم، وقضت المحكمة حضورياً بجلسة 19 من يونيو سنة 2007م بقبول الاستئناف شكلاً، وتأييد الحكم المستأنف فيما قضى به بالنسبة للتهمة الأولى (والتي ارتكبها على متن أحد السفن)، وإلغاء

الأحكام والحكم ببراءة المتهم عن باقي التهم، وذلك أن حدود تطبيق النص الجنائي تتفق وحدود الإقليم الخاضع لسيادة الدولة، فهو يطبق على كل جريمة تُرتكب في هذا الإقليم، ويشمل إقليم الدولة أراضيها وبحرها الإقليمي وفضاءها الجوي، بما في ذلك طبقات الأرض، وإلى مركز الكرة الأرضية، وطبقات الجو والمياه إلى ما لا نهاية في الارتفاع، وهذا الأصل هو الذي أخذ به التشريع الجنائي لدولة الإمارات، إذ نصت المادة (1/16) الواردة في الفصل الثاني من الباب الثاني من الكتاب الأول من قانون العقوبات على "تسري أحكام هذا القانون على كل من يرتكب جريمة في إقليم الدولة، ويشمل إقليم الدولة أراضيها وكل مكان يخضع لسيادتها بما في ذلك المياه الإقليمية والفضاء الجوي الذي يعلوها، كما حرص قانون العقوبات على سريان تلك القاعدة على التشريعات العقابية الأخرى إلا في حالة أن تتضمن نصاً على خلاف ذلك بما أورده في المادة الثالثة منه، والتي نصت على "تسري أحكام الكتاب الأول من هذا القانون على الجرائم المنصوص عليها في القوانين العقابية الأخرى ما لم يرد نص فيها على خلاف ذلك"، بما مفاده أنه إذا ورد نص في أي من تلك القوانين يبسط سريانه من حيث المكان أو الأشخاص – أو غير ذلك – على ما يجاوز المكان الذي يخضع لسيادتها أو الأشخاص الذين يسري عليهم فإنه يكون نافذاً، وكذا الحال إذا قلص نص نطاق سريان القانون من حيث المكان أو الأشخاص.

فلهذه الأسباب حكمت المحكمة بقبول الطعن شكلاً وفي الموضوع برفضه، وألزمت الطاعن بالرسوم القضائية وأمرت بمصادرة التأمين.[41]

(41) الطعن 16 لسنة 2 ق، محكمة تمييز رأس الخيمة الدائرة الجزائية، جلسة 2007/10/21.

المطلب الثاني

أنواع الجرائم الإلكترونية الماسة بأمن الدولة الداخلي

سيتم في هذا المطلب تناول جميع الجرائم التي من شأنها المساس بأمن الدولة الداخلي، والمنصوص عليها في المرسوم بقانون رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، والتي تشمل جرائم الدخول بدون تصريح بقصد الحصول على بيانات حكومية، وجرائم إثارة الفتنة أو الكراهية، وجرائم تعريض مصالح الدولة العليا للخطر، وجرائم الدعوة لقلب نظام الحكم، وجرائم عدم الانقياد للقوانين والأنظمة المعمول بها في الدولة، وجرائم الدعوة للمظاهرات دون ترخيص، وجرائم السخرية أو الإضرار بسمعة وهيبة الدولة، كما سيتم بيان السلوك الإجرامي لكل منها، وأسباب التشديد فيها.

وقد تم تقسيم هذا المطلب لخمسة فروع، تناول كل فرع إحدى هذه الجرائم، وذلك على النحو التالي:

- **الفرع الأول: جرائم الدخول بدون تصريح بقصد الحصول على بيانات حكومية.**
- **الفرع الثاني: جرائم إثارة الفتنة أو الكراهية أو العنصرية أو الإضرار بالوحدة الوطنية أو السلم الاجتماعي.**
- **الفرع الثالث: الجرائم المتعلقة بتعريض أمن الدولة ومصالحها للخطر والمساس بالنظام العام.**
- **الفرع الرابع: الجرائم المتعلقة بالسخرية أو الإضرار بسمعة وهيبة ومكانة الدولة أو أي من مؤسساتها أو رئيسها وحكامها أو أولياء عهودها أو علمها أو سلامها الوطني أو رموزها.**
- **الفرع الخامس: الجرائم المتعلقة بقلب نظام الحكم في الدولة أو الاستيلاء عليه أو تعطيل أحكام الدستور أو القوانين السارية في البلاد.**

الفرع الأول

جرائم الدخول بدون تصريح بقصد الحصول على بيانات حكومية

تتم جرائم الاعتداء على المواقع الإلكترونية أو الأنظمة أو الشبكات أو الوسائل التقنية الخاصة بالمعلومات والبيانات الإلكترونية من خلال صورتين، الأولى صور بسيطة، والثانية صور غير بسيطة، وتتمثل الصور البسيطة في الدخول على موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة[42]، وتتمثل الصور غير البسيطة في حالتين:

الحالة الأولى: بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية.

الحالة الثانية: إذا تعرضت هذه البيانات أو المعلومات للإلغاء أو الحذف، أو الإتلاف أو التدمير، أو الإفشاء أو التغيير، أو النسخ أو النشر أو إعادة النشر.

وتتجسد هذه الجنايات في جريمة الدخول بدون تصريح، والإضرار ببيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية، سواءً تمثل الإضرار في الإلغاء أو الحذف، أو الإتلاف أو التدمير، أو الإفشاء أو التغيير، أو النسخ أو النشر أو إعادة النشر، وقد اعتبر المشرع هذا الإضرار ظرفاً مشدداً.[43]

(42) عبد الرزاق الموافي عبد اللطيف، شرح قانون مكافحة تقنية المعلومات، معهد دبي القضائي، دبي، 2014، ص 42.

(43) عبد الرزاق الموافي عبد اللطيف، شرح قانون مكافحة تقنية المعلومات، المرجع السابق ، ص 43.

وقد نصت المادة (4) من المرسوم بقانون رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات على "يعاقب بالسجن المؤقت والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تتجاوز مليون وخمسمائة ألف درهم كل من دخل بدون تصريح إلى موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلوماتية أو وسيلة تقنية معلومات، سواءً كان الدخول بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية. وتكون العقوبة السجن مدة لا تقل عن خمس 5 سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز 2 مليون درهم، إذا تعرضت هذه البيانات أو المعلومات للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر".

من خلال هذه المادة يتضح أن المشرع قد شدد العقوبة سعياً لضمان حماية وسلامة البيانات الحكومية من عبث الاختراق أو التدمير أو ما شابه ذلك، فمحل الجريمة الذي وضعه المشرع هو البيانات الحكومية، ويُقصد بالبيانات الحكومية البيانات أو المعلومات الإلكترونية الخاصة أو العائدة للحكومة الاتحادية أو الحكومات المحلية لإمارات الدولة، أو الهيئات العامة أو المؤسسات العامة الاتحادية أو المحلية.[44]

الحماية القانونية:

فرض المشرع الحماية لتشمل جميع البيانات الحكومية بأي شكل كانت وباختلاف درجاتها، سواءً كانت سريه أم غير سرية بحسب الدرجات المتعارف عليها من سرية للغاية إلى درجة محظور، ولم يشترط نص المرسوم بقانون السرية بالنسبة للبيانات الحكومية، وجاز أن تتعلق هذه البيانات بأمور مالية

(44) المادة (1) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 وفقاً لأحدث التعديلات بقانون اتحادي رقم 2 لسنة 2018 في شأن قانون مكافحة جرائم تقية المعلومات.

أو تجارية أو اقتصادية، وما دام محل هذه الصورة من التجريم هو مستندات أو بيانات حكومية، فإن ذلك يعني أن الأمر يتعلق بأي وثائق تتضمن بيانات على قدر كبير من الأهمية لصالح الدولة.[45]

السلوك الإجرامي والعلاقة السببية:

بناء على ما سبق فإن السلوك الإجرامي في هذه الجريمة يتمثل بالإفشاء أو النشر أو إعادة النشر والإفشاء دائماً متعلق بسر، ويكون الاعتداء منصباً على بيانات أو معلومات إلكترونية تعود للحكومة الاتحادية أو المحلية لإمارات الدولة، أو إحدى هيئاتها أو مؤسساتها التي تعود طبيعة سرية عملها بموجب الترخيص الصادر لها من جهة الاختصاص في الدولة.[46]

وتنشئ العلاقة السببية بين قيام الجاني بالدخول دون تصريح إلى موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلوماتية أو وسيلة تقنية معلومات، وبين نشر أو إعادة نشر تلك المعلومات والبيانات، إذ لابد وأن يكون الإفشاء أو النشر أو إعادة النشر شرطاً مرتبطاً بالدخول إلى الموقع الإلكتروني أو نظام المعلومات الإلكتروني أو الشبكة المعلوماتية أو أي من وسائل تقنية معلومات، وإلا فلا تطبق حينها أحكام المادة (4) من المرسوم بقانون اتحادي في شأن مكافحة جرائم تقنية المعلومات.[47]

تشديد العقوبة:

ولكي تقوم هذه الجريمة بصورتها المشددة، فإنه لابد من ارتكاب فعل الدخول، ووقوع إضرار فعلي بالبيانات الحكومية، أو بمعلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية في أي صورة من

(45) عبد الرزاق الموافي عبد اللطيف، شرح قانون مكافحة تقنية المعلومات، المرجع السابق، ص 40.
(46) حوراء موسى، الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، دار النهضة العربية، القاهرة، 2018، ص264.
(47) رشدي محمد علي، الحماية الجنائية الموضوعية للمعلومات عبر شبكة الإنترنت، دار النهضة العربية، القاهرة، 2013، ص 310.

الصور التي وردت في نص المادة (4) من هذا القانون، وهي الإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر.

وتتميز الأفعال الواردة في الفقرة الثانية من المادة (4) من المرسوم بقانون والتي تُعد ظروفاً مشددة، بأن وقوع أي فعل منها يكفي للتشديد، حيث لا يلزم أن تقع كلها، كما أن وقوع أكثر من فعل من هذه الأفعال والنتائج لا يترتب عليه تعدد الظروف المشددة، بل يتوافر بها ظرف واحد فقط، وتُعد هذه الأفعال المنصوص عليها في الفقرة الثانية نتائج السلوك الوارد في الفقرة الأولى من المادة (4)، وُتعد صورة التجريم الواردة في الفقرة الثانية من المادة (4) من المرسوم بقانون ضمن طائفة الجرائم المشددة بحدوث النتيجة.

ويتخذ الركن المعنوي صورة العمد والقصد الجنائي في ارتكاب الجريمة، سواءً بالإفشاء أو بالنشر أو إعادة النشر، حيث لا يمكن تصور ارتكاب الجريمة عن طريق الخطأ، كون السلوك فيها لا يمكن أن يتحقق دون وجود قصد جنائي.[48]

ويرى الباحث أن المادة بصفتها المشددة هنا، وأنه من الأفضل دمج الفقرتين الأولى والثانية مع بعضهما البعض في صورة التخفيف والعقوبة التي لا تتجاوز مدة معينة، وأن يكون التشديد بأن لا تقل العقوبة عن فترة محددة في حال نتج عن ذلك ضرراً بمصالح تمس الدولة وكيانها، وذلك من منظور التوازن بين العقوبات التي فرضها المشرع.

(48) حوراء موسى، الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، المرجع السابق، ص 268.

الفرع الثاني

جرائم إثارة الفتنة أو الكراهية أو العنصرية أو الإضرار بالوحدة الوطنية أو السلم الاجتماعي

لقد أصبحت السلوكيات التي من شأنها إثارة الفتنة بين أفراد المجتمع، وتعمل على خلق وتغذية الكراهية والعنصرية والطائفية بين الأفراد من أكثر الأساليب ضرباً للوحدة الوطنية وتشتيتها وتدميرها، الأمر الذي من شأنه الإضرار بالوحدة الوطنية والسلم الاجتماعي، والإخلال بالنظام العام والآداب العامة، وتدمير البنيان الاجتماعي.

وقد نصت المادة (24) من المرسوم بقانون رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات على هذه الصور على أن "يعاقب بالسجن المؤقت والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز مليون درهم كل من أنشأ أو أدار موقعاً إلكترونياً أو أشرف عليه أو نشر معلومات على شبكة معلوماتية أو إحدى وسائل تقنية المعلومات للترويج أو التحبيذ لأي برامج أو أفكار من شأنها إثارة الفتنة أو الكراهية أو العنصرية أو الطائفية أو الإضرار بالوحدة الوطنية أو السلم الاجتماعي أو الإخلال بالنظام العام أو الآداب العامة".[49]

ومن الملاحظ استخدام شبكة الإنترنت وغيرها من وسائل تقنية المعلومات في الترويج لبرامج وأفكار من شأنها إثارة الفتنة، وذلك كما وصفتها المادة أعلاه، خاصة في ظل تواجد الفئات التي تعمل على زرع الكراهية والعنصرية، بما يتنافى مع مبادئ التسامح والتعايش، خاصة بعد انتشار وسائل التواصل

(49) المادة (24) من المرسوم بقانون 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات.

الاجتماعي والتي ساهمت في إفراغ ما في القلوب من شحنات سلبية مكبوتة لدى البعض، فيختبؤون خلف الشاشات الإلكترونية خوفاً من المواجهة.[50]

الحماية القانونية:

وبنص المادة (24) من المرسوم، فقد قام المشرع الإماراتي بفرض الحماية من أجل تجريم إنشاء أو إدارة موقع إلكتروني أو الإشراف عليه، أو نشر معلومات بقصد الترويج أو التحبيذ لتلك البرامج والأفكار التي من شأنها نشر السلوك الإجرامي الذي وصفه المشرع، ولها عدة صور تتمثل في إنشاء أو إدارة موقع إلكتروني أو الإشراف عليه، وكذلك نشر معلومات على شبكة معلوماتية أو إحدى وسائل تقنية المعلومات، ولكن يجب أن يكون الموقع والنشر للترويج أو التحبيذ لبرامج أو أفكار معينة، فسلوك المجرم هو الإنشاء أو الإدارة أو الإشراف أو النشر، ولا يلزم ارتكابها جميعاً، حيث يكفي الإتيان بسلوك واحد منها لأخذ صور التجريم.[51]

السلوك الإجرامي والعلاقة السببية:

وللترويج لبرامج وأفكار معينة، وذلك إتباع أساليب تنطوي على الدعاية لها، وليس فقط مجرد نقل الأخبار بشأنها، ويقع هذا الترويج سواءً بالقول أو الكتابة أو أي وسيلة أو طريقة أخرى من طرق العلانية التي يكون من شأنها تحقق الترويج. أما تحقق التحبيذ فيكون من خلال المدح والتفضيل والاستحسان، أي بالنظر إليها بالقبول والملائمة.

ويؤدي الإضرار بالوحدة الوطنية والسلم الاجتماعي لزعزعة وشق وحدة المجتمع، وإضعاف انتماء الأفراد للدولة، لأن السلم الاجتماعي يعمل على توثيق العلاقات بين أفراد المجتمع وفئاته مهما تنوعت دينياً وعرقياً وثقافياً وسياسياً، وذلك على أسس من الاستقرار والطمأنينة، والاحترام المتبادل بين فئات

(50) حوراء موسى، الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، المرجع السابق، ص 284.
(51) حوراء موسى، الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، المرجع السابق، ص 286.

المجتمع وقطاعاته المتنوعة، والإضرار به يعني انتشار النزاعات والخصومات الاجتماعية المختلفة، والاحتكام إلى العنف في التعاملات وحل الخلافات، وبفقدان حالة السلم الاجتماعي أو ضعفها فإن النتيجة الطبيعية هي تدهور الأمن، وزعزعة الاستقرار، وعدم تحقيق التنمية والتقدم للمجتمع والوطن معاً.

وتُعتبر الجريمة في المادة (24) من قانون مكافحة جرائم تقنية المعلومات داخلة في طور العمد، كونها تأخذ صورة القصد الجنائي العام، والذي يقوم على عنصر الإرادة والعلم، والركن المعنوي للجريمة يقوم بعلم الجاني بكافة عناصر الجريمة، بأن يعلم أنه قام بإنشاء موقع الإلكتروني أو أدار أو أشرف عليه، أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، وأن يعلم بأن السلوك الذي يصدر عنه فيه ترويج أو تحبيذ لبرامج وأفكار من شأنها إثارة الفتنة أو الكراهية أو العنصرية أو الطائفية، أو الإضرار بالوحدة الوطنية أو السلم الاجتماعي، أو الإخلال بالنظام العام أو الآداب العامة.

ويمكن تمثيل علم الجاني أثناء نشره بأن المواد التي يقوم بنشرها على الشبكة المعلوماتية أو وسائل تقنية المعلومات تحث على الكراهية والطائفية؛ أي أنه يجهل طبيعتها التحريضية على الكراهية والطائفية، ويجب أن تتجه إرادة الجاني إلى الترويج أو التحبيذ لتلك البرامج والأفكار التي من شأنها إثارة الفتنة أو الكراهية أو العنصرية أو الطائفية، أو تحث على الكراهية والطائفية وذلك دون إكراه.[52]

تشديد العقوبة:

شدد المشرع العقوبة بنصه بعقوبة السجن المؤقت بدلاً من الحبس الذي كان ينص عليه القانون القديم، وأضاف للعقوبة الغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز مليون درهم، وعلى القاضي أن يحكم بالسجن والغرامة أي بجمع العقوبتين معاً؛ حيث لا سلطة تقديرية للقاضي في هذا

(52) عبد الرزاق الموافي عبد اللطيف، شرح قانون مكافحة تقنية المعلومات، المرجع السابق، ص 54.

الشأن، وإلا كان الحكم معيباً، أما تحديد مدة السجن فإنها تخضع للقواعد العامة، فلا تقل عن ثلاث سنوات، ولا تزيد على خمس عشرة سنة.

وبالإضافة إلى العقوبات السابقة يُحكم بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب هذه الجريمة، أو الوسائل المتحصلة منها، وكذلك بإغلاق المحل أو الموقع الذي ارتكبت منه الجريمة، سواءً كانت الجريمة قد ارتكبت بعلم مالكه أم دون علمه، وأن يكون الإغلاق كلياً أو للمدة التي تقدرها المحكمة.

الفرع الثالث

الجرائم المتعلقة بتعريض أمن الدولة ومصالحها للخطر والمساس بالنظام العام

يستخدم البعض الشبكات الإلكترونية وشبكة الإنترنت أو مواقع التواصل الاجتماعي في التحريض على أفعال أو نشر أو بث معلومات أو أخبار أو رسوم كرتونية أو أي صور أخرى من شأنها تعريض أمن الدولة ومصالحها العليا للخطر، أو المساس بالنظام العام، أو الاعتداء على مأموري الضبط القضائي أو أي من المكلفين بتنفيذ أحكام القانون، وفيما يتعلق بنشر الأخبار الكاذبة، فمن الممكن مثلاً نقل أو نشر أخبار عن تواجد عصابة مسلحة في الدولة، أو نشر إشاعة تعرض الدولة للحرب أو الاحتلال أو حدوث انفجارات، أو نشر خبر كاذب من خلال مقاطع فيديو عن حدوث اعتداءات مسلحة، ويدعي الجاني في مثل هذه الأخبار الكاذبة أنها حدثت بالدولة، بينما في الواقع هي أحداث تمت في دولة أخرى، بل وربما في زمن آخر[53].

الحماية القانونية:

هذه الجرائم من الممكن أن ترتكب عبر شبكة الإنترنت بما فيها وسائل التواصل الاجتماعي، وقد جَرّم المشرع هذه الصور في المادة (28) من المرسوم بقانون رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، حيث نصت على "يعاقب بالسجن المؤقت والغرامة التي لا تجاوز مليون درهم كل من أنشأ أو أدار موقعاً إلكترونياً أو أشرف عليه أو استخدم معلومات على الشبكة المعلوماتية أو وسيلة تقنية معلومات بقصد التحريض على أفعال، أو نشر أو بث معلومات أو أخبار أو رسوم كرتونية أو

(53) حوراء موسى، الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، المرجع السابق، ص 294.

أي صور أخرى من شأنها تعريض أمن الدولة ومصالحها العليا للخطر، أو المساس بالنظام العام، أو الاعتداء على مأموري الضبط القضائي أو أي من المكلفين بتنفيذ أحكام القوانين".[54]

وقد استحدثت هذه المادة جريمة الإنشاء أو الإدارة لموقع إلكتروني أو الإشراف عليه بقصد التحريض على أفعال أو نشر أو بث معلومات أو أخبار أو رسوم كرتونية أو أي صور أخرى من شأنها تعريض أمن الدولة ومصالحها العليا للخطر، أو المساس بالنظام العام.

السلوك الإجرامي:

جَرّم المشرع إنشاء أو إدارة موقع إلكتروني أو الاشراف عليه، أو استخدام معلومات على الشبكة المعلوماتية أو وسيلة تقنية معلومات، أو نشر أو بث معلومات أو أخبار أو رسوم كرتونية أو أي صور أخرى يكون من شأنها تعريض أمن الدولة ومصالحها للخطر، أو المساس بالنظام العام.

ويُلاحظ من هذا النص وجود ثلاثة أنواع للسلوك الإجرامي، هي على النحو التالي:

1) إنشاء أو إدارة موقع إلكتروني أو الإشراف عليه بقصد التحريض على أفعال من شأنها تعريض أمن الدولة ومصالحها للخطر، أو المساس بالنظام العام؛ فمحل السلوك المُجَرَم هنا هو الموقع الإلكتروني.
2) استخدام معلومات على الشبكة المعلوماتية أو وسيلة تقنية معلومات بقصد التحريض على أفعال من شأنها تعريض أمن الدولة ومصالحها للخطر، أو المساس بالنظام العام؛ ويقصد

(54) المادة (28) من المرسوم بقانون 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، هذه المادة معدلة بموجب المرسوم بقانون اتحادي رقم (2) لسنة 2018 في شأن تعديل بعض مواد المرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

باستخدام المعلومات الانتفاع بها واستغلالها في الجرائم؛ فمحل الاستخدام هنا هو المعلومات[55].

3) نشر أو بث معلومات أو أخبار أو رسوم كرتونية أو أي صور أخرى من شأنها تعريض أمن الدولة ومصالحها العليا للخطر، أو المساس بالنظام العام، محل الاستخدام هنا هو نشر وبث المعلومات أو الأخبار أو الرسوم الكرتونية أو أي صور أخرى.[56]

الركن المعنوي:

هو القصد الجنائي كون السلوك الإجرامي في هذا النص يأخذ صورة الجريمة العمدية، يتضمن تحريضا[57]، وأن يعلم بأن تحريضه من شأنه تعريض أمن الدولة ومصالحها العليا للخطر أو المساس بالنظام العام، ويجب أن تتجه إرادته إلى السلوك المتمثل في إنشاء أو إدارة موقع إلكتروني أو الإشراف عليه، واستخدم معلومات على الشبكة المعلوماتية أو وسيلة تقنية معلومات، نشر أو بث معلومات أو أخبار أو رسوم كرتونية أو أي صور أخرى.[58]

وتعني المصالح العليا للدولة المصلحة القومية المرتبطة بكل ما يتعلق بمصالح الدولة، سواءً من الناحية التي تختص بالمرافق العامة، أو نظام الحكم، أو من الناحية الحربية أو السياسية أو الاقتصادية،

---

(55) يُقصد بالمعلومات تلك البيانات التي تمت معالجتها بحيث أصبحت ذات معنى، وصارت مرتبطة بسياق معين، ومثال ذلك المعلومات السياسية، وهي المعلومات المرتبطة بسياق سياسي، والمعلومات الاقتصادية وهي المرتبطة بسياق اقتصادي....إلخ.

(56) يُقصد بالأخبار: ما يُنقل من معلومات وأحداث ويتحدث بها قوة، أو كتابة الخبر قول يحتمل الصدق والكذب لذاته. هي المعلومات التي تتعلق بحادث معين، وترتكز أو تبدو أنها مرتكزة على الواقع المادي، فلا يدخل فيها التخمينات المستقبلية أو التنبؤات، فلفظ خبر ينبغي أن يكون متعلقاً بأمر قريب من جهة تصور حصوله، أي أن الواقعة حدثت أو ستحدث في وقت قصير من إذاعة نبئها.

(57) خلق التصميم على الجريمة لدى الفاعل الأصلي لدفعه حول ارتكابها، وينصب التحريض على أفعال من شأنها تعريض أمن الدولة ومصالحها العليا للخطر، أو المساس بالنظام العام.

(58) عبد الرزاق الموافي عبد اللطيف، شرح قانون مكافحة تقنية المعلومات، المرجع السابق، ص 74.

ومن أمثلة ذلك التآمر على إحداث اضطرابات داخلية، أو عمل مشروعات اقتصادية تؤدي لإلحاق الضرر بالدولة، سواءً كانت الأضرار سياسية أو اقتصادية أو اجتماعية أو أمنية أو ثقافية.

ويلي الإضرار بالمصالح العليا للدولة إلحاق الضرر بالنظام العام، وهو ما يؤدي بطبيعة الحال لضرر مباشر بالمجتمع، مثل الإضرار بالأمن العام والصحة العامة والسكينة المجتمعية؛ والتي يتجه إليها القصد الجنائي من خلال السلوك الإجرامي الذي صدر عن المجرم، ويحدث الإخلال بالنظام العام في حالة فقد الأفراد للطمأنينة والأمان، أو المساس بالهدوء المجتمعي والصحة العامة.

وفي النهاية فإن التجريم المنصوص عليه في المادة (28)، والمتمثل في إنشاء أو إدارة موقع إلكتروني أو الإشراف عليه بقصد التحريض على أفعال من شأنها تعريض أمن الدولة ومصالحها للخطر أو المساس بالنظام العام، وكذلك المتمثل في جريمة استخدام معلومات الشبكات أو تقنيه المعلومات، أو بث أخبار أو رسوم كرتونية أو أي صور أخرى من شأنها تعريض أمن الدولة ومصالحها العليا للخطر، أو المساس بالنظام العام.[59]

وعاقب المرسوم الجديد على هذه الجرائم بالسجن المؤقت، والذي تُحَدَد مدته وفقاً للقواعد العامة بأن لا تقل عن ثلاث سنوات ولا تزيد على خمس عشرة سنة، بالإضافة إلى الغرامة التي لا تتجاوز مليون درهم، والجمع بين السجن والغرامة وجوبي وإلا كان الحكم معيباً، وليس للقاضي سلطة تقديرية في هذا الشأن، أما بالنسبة للتدابير التي يلتزم القاضي بالإشارة إليها في الحكم، فسوف يتم التطرق إليها في الفصل الثاني.

(59) عبد الرزاق الموافي عبد اللطيف، شرح قانون مكافحة تقنية المعلومات، المرجع السابق، ص 76.

الفرع الرابع

الجرائم المتعلقة بالسخرية أو الإضرار بسمعة وهيبة ومكانة الدولة أو أي من مؤسساتها أو رئيسها أو حكامها أو أولياء عهودها أو علمها أو سلامها الوطني أو رموزها

يحرص كل مواطن غيور على وطنه للحفاظ على سمعته وهيبتها، وتربطه بها رابطة الجنسية والولاء، وهذا أمر طبيعي ومُفْتَرَض لدى جميع المواطنين، حيث يجب أن يتحلى كل مواطن بالمسؤولية تجاه وطنه، ويبذل قصارى جهده لحمايته، ويسعى لتحقيق أمنه واستقراره.

ولكن انتشرت وتعددت في الأونة الأخيرة سلوكيات تهدف لنشر معلومات وأخبار وبيانات وإشاعات تمس بسمعة أو هيبة أو مكانة الدولة أو أي مؤسساتها، أو رئيسها أو حكامها أو أولياء عهودها أو نوابهم، أو علمها أو سلامها الوطني، وذلك عبر تقنية المعلومات أو الشبكة المعلوماتية، سواءً من خلال مواقع إلكترونية أو مواقع التواصل الاجتماعي، الأمر الذي حدى بالمشرع لتجريم هذه السلوكيات، نطراً لجسامة الأضرار المباشرة الناتجة عنها فيما يتعلق بسمعه وهيبة الدولة، وانعكاس ذلك على تكدير الأمن العام، لأن مثل هذه الأمور تؤثر على مقومات الدولة سلبياً، وبالتالي كان لابد من تجريمها، وسن تشريعات تعاقب عليها، حيث تمثل حماية الدولة بكل مكوناتها السياسية والاقتصادية والاجتماعية الأولوية عن أي مصلحة أخرى، فباستقرار الوطن يستقر المجتمع ويستقر جميع أفراده.

وهذه الجرائم من الممكن أن ترتكب عبر شبكة الإنترنت بما فيها المواقع الإلكترونية أو مواقع التواصل الاجتماعي[60]، وقد جَرّمها المشرع في المادة (29) من المرسوم بقانون رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، حيث نصت على "يعاقب بالسجن المؤقت والغرامة التي

(60) حوراء موسى، الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، المرجع السابق، ص 306.

لا تجاوز مليون درهم كل من نشر معلومات أو أخبار أو بيانات أو إشاعات على موقع إلكتروني أو أي شبكة معلوماتية أو وسيلة تقنية معلومات بقصد السخرية أو الإضرار بسمعة أو هيبة أو مكانة الدولة أو أي مؤسساتها أو رئيسها أو نائبه أو حكام الإمارات أو أولياء عهودهم أو نواب حكام الإمارات أو علم الدولة أو السلام الوطني أو شعارها أو نشيدها الوطني أو رموزها".

السلوك الإجرامي:

يتمثل السلوك الإجرامي هنا في نشر معلومات أو أخبار أو بيانات أو إشاعات عبر أي الشبكات المعلوماتية أو وسائل التواصل الاجتماعي، والتي تعتبر بمثابة أداة للجريمة، ويُقصد بالنشر الإذاعة أو الاشاعة سواءً عبر صور إلكترونية أو فوتوغرافية، أو مشاهد أو تعليقات أو بيانات يسعى إليها الجاني ليطلع الجمهور أو الرأي العام عليها.[61]

الركن المعنوي:

تُعد هذه الجريمة من الجرائم العمدية بقصد، ويلزم بها العلم والإرادة من النشر، وذلك بتضمن سلوكه السخرية والإضرار بسمعة الدولة أو مكانتها أو منزلتها بحسب وصف المادة.

(61) عبد الرزاق الموافي عبد اللطيف، شرح قانون مكافحة تقنية المعلومات، المرجع السابق، ص 78.

الفرع الخامس

الجرائم المتعلقة بقلب نظام الحكم في الدولة أو الاستيلاء عليه أو تعطيل أحكام الدستور أو القوانين السارية في البلاد

تحرص جميع الدول إلى الحفاظ على نظامها السياسي وحمايته من أي اعتداء مهما كان الشكل السياسي للدولة، الأمر الذي جعل المشرع يُجَرِم أي محاولة للمساس بنظام الحكم، حتى ولو كان بمجرد الدعوة لذلك، وحتى وإن لم يترتب على الدعوة أية آثار للخروج على الحاكم، وتمتد هذه الحماية لتشمل التصدي لتعطيل الدستور أو والقوانين السارية في البلاد.[62]

وتنشأ الدعوة لقلب أو تغيير نظام الحكم في البلاد أو الاستيلاء عليه بداية من خلال التحريض على ذلك، ثم اتباع أساليب تهدف لكراهيته وازدرائه، وذلك من خلال بث فكرة تغيير النظام القائم في نفوس المواطنين، ودعوتهم لازدرائه، حتى تسوقهم تلك الفكرة إلى السعي نحو تغييره أو الاستيلاء عليه، سواءً كانت الغاية من قلب نظام الحكم أو الاستيلاء عليه جزئياً كان أو كلياً.[63]

ويُعد من قبيل الدعوة أو التحريض أو الترويج لقلب أو تغيير نظام الحكم أو الاستيلاء عليه تحريض الغير على تغيير الحكم الرئاسي إلى حكم جمهوري، على أن تكون العبارات دالة على وجوب اتخاد سلوك يحارب النظام القائم، ونظراً لإمكانية ارتكاب هذه الجرائم عبر تقنية المعلومات أو شبكات التواصل الاجتماعي، فقد جَرّمها المشرع ونص عليها في المادة (30) من المرسوم بقانون رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، حيث نصت على "يعاقب بالسجن المؤبد كل من أنشأ أو أدار موقعاً إلكترونياً أو أشرف عليه أو نشر معلومات على الشبكة المعلوماتية أو وسيلة تقنية معلومات

(62) طارق سرور، جرائم النشر والإعلام، دار النهضة العربية، القاهرة، الطبعة الأولى، 2004، ص 366.
(63) حوراء موسى، الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، المرجع السابق، ص 319.

تهدف أو تدعو إلى قلب أو تغيير نظام الحكم في الدولة أو الاستيلاء عليه أو إلى تعطيل أحكام الدستور أو القوانين السارية في البلاد أو المناهضة للمبادئ الأساسية التي يقوم عليها نظام الحكم في الدولة، ويعاقب بالعقوبة ذاتها كل من روج إلى أو حرض على أي من الأفعال المذكورة أو سهلها للغير".

السلوك الإجرامي:

يتمثل السلوك الإجرامي لهذه الجريمة عدة صور، ويكفي ارتكاب إحداها لقيام الجريمة وهي (1. إنشاء أو إدارة موقع إلكتروني أو الإشراف عليه، ٢. نشر معلومات على الشبكة المعلوماتية أو وسيلة تقنية معلومات، ٣. الترويج لقلب أو تغيير نظام الحكم في الدولة أو الاستيلاء عليه أو إلى تعطيل أحكام الدستور أو القوانين السارية في البلاد أو المناهضة للمبادئ الأساسية التي يقوم عليها نظام الحكم في الدولة. 4. التحريض على أي من الأفعال المذكورة، 5. تسهيل أي من الأفعال المذكورة للغير).[64]

الركن المادي:

يكمن الركن المادي لهذه الجريمة في إنشاء موقع أو إدارته على شبكة تقنية المعلومات أو إحدى مواقع التواصل الاجتماعي، وذلك للغايات المنصوص عليها في المادة أعلاه، بغض النظر عن تحققها من عدمه، كونها جريمة شكلية وليست جريمة مادية، ولا يلزم أن تتحقق الدعوة إلى قلب أو تغيير نظام الحكم في الدولة أو الاستيلاء عليه، أو إلى تعطيل أحكام الدستور أو القوانين السارية في البلاد، أو المناهضة للمبادئ الأساسية التي يقوم عليها نظام الحكم في الدولة، كما لا يلزم تحقق وجود خطر حقيقي في الأصل بمجرد الدعوة، أو التحريض على قلب نظام الحكم.[65]

(64) عبد الرزاق الموافي عبد اللطيف، شرح قانون مكافحة تقنية المعلومات، المرجع السابق، ص 75.

(65) حوراء موسى، الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، المرجع السابق، ص 324.

ويتجسد الركن المعنوي لهذه الجريمة في القصد الجنائي كونها جريمة عمدية، ويلزم لقيامها القصد الجنائي بالعلم والإرادة؛ فيجب أن يعلم الجاني بأنه ينشئ أو يدير موقعاً إلكترونياً أو يشرف عليه، وبأنه ينشر معلومات على الشبكة المعلوماتية أو وسيلة تقنية معلومات.

كما يجب أن يعلم بأن سلوكه يتضمن دعوة أو يهدف إلى قلب أو تغيير نظام الحكم في الدولة أو الاستيلاء عليه، أو إلى تعطيل أحكام الدستور أو القوانين السارية في البلاد، أو المناهضة للمبادئ الأساسية التي يقوم عليها نظام الحكم في الدولة.[66]

ويجب أن تتجه إرادته إلى الإنشاء أو الإدارة أو الإشراف على الموقع، وإلى نشر تلك المعلومات على الشبكة المعلوماتية أو وسيلة تقنية معلومات، وأن تتجه إرادته أيضاً إلى تلك الدعوة والهدف منها.

وقد فرض المشرع بحسب نص المادة أعلاه عقوبة السجن المؤبد بالإضافة لمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب هذه الجريمة أو الأموال المتحصلة منها، واغلاق المحل أو الموقع الذي أُرتكبت فيه الجريمة كلياً أو للمدة التي تصدرها المحكمة، وللمحكمة أن تقضي بإبعاد الأجنبي الذي يحكم عليه بالإدانة، وللمحكمة مراعاة أي عقوبة أشد يُنَص عليها في أي قانون آخر.

كما نصت المادة على مجموعة من التدابير التي يجوز للمحكمة الحكم بها، فقد نصت على تدبير وضع المحكوم عليه تحت الإشراف أو المراقبة، وحرمانه من استخدام أي شبكة معلوماتية، أو استخدام نظم المعلومات الإلكترونية، أو أي وسيلة تقنية معلومات أخرى، بالإضافة لتدبير وضعه في مأوى علاجي أو مركز تأهيل، وأن تحدد المدة التي تراها المحكمة مناسبة لذلك، وهو ما سيتم التطرق له تفصيلاً في الفصل الثاني.

(66) حوراء موسى، الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، المرجع السابق، ص 324.

المبحث الثاني

الجرائم الإلكترونية الماسة بالأمن الخارجي

تلتقي الجرائم الماسة بأمن الدولة الداخلي والخارجي بأحكام مشتركة يمكن تلخيصها بالاختصاص العيني والاختصاص القضائي، والتوسع في تحديد جرائم الخطر، وفي التحريض والاتفاق الجنائي، وصفة مرتكبي الجرائم، وكذلك من حيث الصياغة التشريعية والقانونية، وفي التجريم والعقوبة، وفي أصول الملاحقة والمحاكمة والمعاقبة، واقتصاص ضمانات حق الدفاع، وتجريم الامتناع عن التبليغ عن بعض الجرائم.[67]

وحسب ما تم بيانه في المبحث الأول فيما يخص الجرائم التي تمس أمن ومصالح الدولة داخلياً، ففي هذا المبحث الأخير من هذا الفصل سيتم تقسيمه لمطلبين، يتناول المطلب الأول شرح نطاق تطبيق القانون على الجرائم الماسة بأمن الدولة ومصالحها في الخارج، وبيان موقف المشرع الإماراتي في هذا الصدد، بينما يتناول المطلب الثاني أنواع الجرائم من حيث أركان الجريمة والتشديد حسب ما نص عليه المرسوم بقانون رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، وذلك على النحو التالي:

- **المطلب الأول: نطاق جرائم أمن الدولة الخارجي.**
- **المطلب الثاني: أنواع الجرائم الإلكترونية الماسة بأمن الدولة الخارجي.**

(67) سعد إبراهيم الأعظمي، موسوعة الجرائم الماسة بأمن الدولة الداخلي، دار الشؤون الثقافية العامة، بغداد، 2000، ص 15.

المطلب الأول

نطاق جرائم أمن الدولة الخارجي

نصت المادة (47) من المرسوم بقانون 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات على "مع عدم الإخلال بأحكام الفصل الثاني من الباب الثاني من الكتاب الأول من قانون العقوبات تسري أحكام هذا المرسوم بقانون على كل من ارتكب إحدى الجرائم الواردة به خارج الدولة إذا كان محلها نظام معلوماتي إلكتروني أو شبكة معلوماتية أو موقع إلكتروني أو وسيلة تقنية معلومات خاصة بالحكومة الاتحادية أو إحدى الحكومات المحلية الإمارات الدولة أو إحدى الهيئات أو المؤسسات العامة المملوكة لأي منهما".

وكما تم التوضيح سلفاً بالاختصاص المكاني في الجرائم الإلكترونية الماسة بالأمن الداخلي، فينطبق على هذه الجرائم نفس النظريات، وإن كان هناك استثناءات وضوابط نص عليها القانون.

ويُعتبر وقوع الجريمة على الإقليم الوطني لدولة الإمارات العربية المتحدة شرطاً جوهرياً لتطبيق قانون العقوبات الاتحادي على هذه الجريمة.

ولا يوجد شك في أن تحديد مكان وقوع الجريمة يتوقف على طبيعة الجريمة نفسها، وعلى نوع النشاط الإجرامي المرتكب من الجاني، وعلى المركز القانوني الذي ينزله القانون على الجاني مرتكب الجريمة، فيما إذا كان فاعلاً أصلياً أم شريكاً فيها، ويمكن القول بأن مكان ارتكاب الجريمة يتحدد بالمكان الذي يتحقق فيه ركنها المادي أو جزء من هذا الركن، فالعبرة إذن بوقوع ماديات الجريمة على إقليم الدولة، وأبسط صورة لذلك أن تقع كافة عناصر الركن المادي على هذا الإقليم، كذلك فإن الجريمة تُعتبر قد وقعت على الإقليم إذا وقع فقط أحد عناصر الركن المادي على هذا الإقليم، كأن يُرْتَكَب السلوك المادي في الإقليم، وتتحقق النتيجة الإجرامية على إقليم آخر.

ووفقا لهذه القاعدة العامة فإن وقوع الركن المادي للجريمة بأكمله، أو وقوع أي عنصر من عناصره الثلاثة (الفعل، النتيجة، العلاقة السببية) على إقليم دولة الإمارات العربية المتحدة يؤدي لتطبيق قانون العقوبات الاتحادي عليها، ويُلاحظ أن العبرة هنا بوقوع الركن المادي للجريمة بكامل عناصره، أو بوقوع أحد عناصره داخل إقليم الدولة؛ لكي يطبق على الجريمة قانون العقوبات الوطني.

ولذلك فإن قانون العقوبات الاتحادي يطبق في تلك الفروض التي قد يكون فيها الجاني خارج إقليم الدولة، ويرتكب أفعالاً في الخارج تجعله فاعلاً أو شريكاً في جريمة وقعت كلها أو بعضها على إقليم دولة الإمارات، ويبدو ذلك في فرضين هما:

الأول: بموجب المادة (19) من قانون العقوبات الاتحادي والتي تنص على "يسرى هذا القانون على كل من ارتكب فعلاً خارج الدولة يجعله فاعلاً أو شريكاً في جريمة وقعت كلها أو بعضها داخل الدولة"، فالجاني إذا كان خارج دولة الإمارات وارتكب فعلاً يجعله فاعلاً أصلياً لجريمة تحققت كل عناصر ركنها المادي أو أحد عناصر هذا الركن داخل إقليم دولة الإمارات، فإنه يطبق على هذه الجريمة في هذه الحالة قانون العقوبات الاتحادي.

الثاني: بموجب أيضاً المادة (19) من قانون العقوبات الاتحادي إذا وقع أي من أفعال الاشتراك (التحريض، الاتفاق، المساعدة) خارج إقليم دولة الإمارات، وارتكب الفاعل الأصلي الجريمة موضوع الاشتراك داخل إقليم دولة الإمارات، فإن قانون العقوبات الاتحادي يطبق في هذه الحالة.

ويُلاحظ أنه إذا وقعت أفعال الاشتراك فقط خارج دولة الإمارات، فلا يطبق قانون العقوبات الاتحادي؛ لأن المشرع اعتد في المادة (19) سالف الإشارة إليها بوقوع الجريمة كلها أو بعضها في إقليم دولة الإمارات.

ويتم تطبيق هذا النص بالنظر إلى طبيعة المصلحة التي يحميها؛ ولذلك فإنه يطبق على كل جريمة تمس مصلحة أساسية للدولة، دون الاعتداد في ذلك بمكان ارتكابها، أو بجنسية مرتكبها، فالضابط في

تحديد سلطان النص الجنائي يكمن في أهمية المصلحة التي تهددها الجريمة، بصرف النظر عن الإقليم الذي ارتكبت فيه، وعن جنسية مرتكبها.

ويمثل هذا المبدأ أهمية واضحة لكل دولة، ذلك أن كل دولة تحرص على حماية مصالحها الأساسية عن طريق إخضاع الجرائم التي تمسها لقانونها الداخلي ولقضائها الوطني، خاصة وأن الدول الأخرى قد لا تهتم بالاعتداءات التي تمس مصالح غيرها؛ وبذلك فإن ضابط المصلحة كأساس لامتداد القانون الوطني خارج إقليم الدولة يُعد هو الأساس لهذا الامتداد، وهو بمثابة توسع في مبدأ الإقليمية؛ فمصالح الدولة الوطنية تحتاج إلى حماية قانونها الوطني، حتى ولو جاء الاعتداء عليها من خارج نطاقها الإقليمي.

وبموجب المادة (٢٠) من قانون العقوبات الاتحادي فإن هذا القانون يمتد خارج إقليم الدولة؛ لكي يطبق على الجرائم التي تمس المصالح الأساسية للدولة، وذلك بصرف النظر من مكان ارتكابها، أو جنسية مرتكبها؛ وبذلك يمكن تحديد الشروط الآتية لتطبيق هذا المبدأ:

1) أن تقع الجريمة التي تمس المصالح الأساسية للدولة خارج نطاقها الإقليمي.
2) أن تكون الجريمة التي تمس المصالح الأساسية للدولة من الجرائم المنصوص عليها في قانون العقوبات الاتحادي، بما فيها الجرائم الماسة بأمن الدولة الخارجي أو الداخلي، أو ضد نظامها الدستوري، أو سنداتها المالية المأذون بإصدارها، أو طوابعها، أو جريمة تزوير أو تقليد محرراتها أو أختامها الرسمية.[68]

ومن خلال هذا النطاق الذي يبين الجريمة التي تقع خارج الدولة وفق موضوع البحث، من حيث إن كيان الدولة المادي والأدبي تجاه الدول الأخرى، وفقدان الدولة لهذا الكيان معناه انهيار الذاتية

(68) علي محمود علي حمودة، قانون العقوبات: النظرية العامة للجريمة، المرجع السابق، ص 90.

المتميزة للشعب وصيرورته، فالجرائم المضرة بأمن الدولة من الخارج هي تلك الجرائم التي تنطوي على الإضرار أو الاعتداء أو المساس باستقلال الدولة أو بسيادتها أو مصالحها القومية، وهذا التعريف يتسع ليشمل جميع أنواع الجرائم التي يتحقق فيها معنى الإضرار بأمن الدولة الخارجي، أو مجرد تعريضه للخطر[69].

وتعد أخطر الأفعال غير المشروعة التي جَرّمها المشرع الإماراتي لحماية أمن الدولة الخارجي هي الجرائم المتعلقة بالجماعات الإرهابية أو الهيئات غير المشروعة، والجرائم المتعلقة بتقديم معلومات غير صحيحة أو غير دقيقة من شأنها الإضرار بمصالح الدولة.[70]

وقد حددت المادة (47) نطاق تطبيق أحكام المرسوم الجديد بقانون، حيث أقرت تطبيق أحكامه على كل شخص يرتكب جريمة من الجرائم المنصوص عليها فيه خارج الدولة، إذا كان محلها نظام معلوماتي إلكتروني، أو شبكة معلوماتية، أو موقع إلكتروني، أو وسيلة تقنية معلومات تخص الحكومة الاتحادية أو إحدى الحكومات المحلية لإمارات الدولة.

ولإيضاح ما سبق حول مبدأ الإقليم، فسيتم نتناول بعض الأحكام القضائية المتعلقة به:

القضية الأولى:

في حكم المحكمة الاتحادية العليا بتاريخ 2003/4/12 بدائرة دبي، رفضت المحكمة الطعن المقدم من المتهم بالإبعاد، لارتكابه جريمة تزوير جواز سفر خارج إقليم دولة الإمارات العربية المتحدة، لكنه استعمله داخل أراضيها، ورفضت دفعه بعدم اختصاص القضاء الوطني بنظر الدعوى الجزائية الماثلة على حسب أن فعل التزوير في جواز السفر المضبوط وقع خارج حدود إقليم الدولة، بما مؤداه عدم

(69) أحمد فتحي سرور، الوسيط في قانون العقوبات، القسم الخاص، المرجع السابق، ص 21.
(70) أحمد غانم سيف السويدي، المواجهة الجنائية والأمنية للجرائم الماسة بأمن الدولة الداخلي، المرجع السابق، ص 15.

سريان قانون العقوبات الإماراتي على هذه الجريمة، لكون الاستعمال هو جريمة بحد ذاته، ومستقلة عن جريمة التزوير نفسها، حيث تنص المادة (16) من قانون العقوبات الاتحادي على "تسري أحكام هذا القانون على كل من يرتكب جريمة في إقليم الدولة. ويشمل إقليم الدولة أراضيها وكل مكان يخضع لسيادتها بما في ذلك المياه الإقليمية والفضاء الجوي الذي يعلوها. وتُعتبر الجريمة مرتكبه في إقليم الدولة إذا وقع فيها فعل من الأفعال المكونة لها أو إذا تحققت فيها نتيجتها أو كان يراد أن تتحقق فيها"، وطلبت المحكم عقاب المتهم بالمواد (6/216 –7، 1/218) من قانون العقوبات الصادر بالقانون الاتحادي رقم 3 لسنه 1987 والمواد (1، 1/2، 28، 31، 33، 34، 36) من القانون الاتحادي رقم 73/6 المعدل بالقانون رقم 13 لسنه 1996 في شأن دخول وإقامه الأجانب.

وإذ كان الثابت أن المتهم استعمل الجواز المزور لدى دخوله إقليم الدولة فإنه يخضع في تجريمه وعقابه لقانون العقوبات الإماراتي ولقضاء الدولة[71].

القضية الثانية:

وفي حكم آخر لمحكمة استئناف دبي، تتلخص وقائع الدعوى بأن المجني عليها تقدمت بشكوى مفادها بأن المتهم قذفها علانية بأن أسند إليها بطريق النشر بموقع صحيفة إيلاف الإلكترونية خبر مفاده سريان شائعات عن وفاة ثري عربي خلال ممارسة الجنس معها بأحد فنداق دبي، مقابل مبلغ مالي كبير، وطالبت النيابة بعقاب المتهم بالمادتين (3/9، 372) من قانون العقوبات الاتحادي رقم 3 لسنة 1987، وقضت محكمة أول درجة غيابياً بعدم اختصاص محكمة دبي بنظر الدعوى، وبعدم قبول الدعوى المدنية، وألزمت رافعها المصروفات، فطعنت النيابة العامة على الحكم السابق بالاستئناف رقم 1248 لسنة 2003 بالتقرير الحاصل في 2003/4/21، وأرفقت به مذكرة طلبت في ختامها إلغاء

(71) المحكمة الاتحادية العليا، طعن رقم (103) لسنة 31 قضائية.

الحكم المستأنف فيما يتعلق بالدعوى المدنية، والحكم المستأنفة وطلباتها، وإلزام المستأنف ضده الرسوم والأتعاب.

وحكمت محكمة النقض بإلغاء الحكم المستأنف بشقيه، وبنت تعليلها في ذلك على أن الحكم المستأنف أسس قضاءه بعدم الاختصاص على سند من القول إن الخبر تم نشره بلندن، وإن إقامة المتهم بلندن. وحيث أن المادة (2/16) من قانون العقوبات قد نصت على "وتُعتبر الجريمة مرتكبة في إقليم الدولة إذا وقع فيها فعل من الأفعال المكونة لها أو إذا تحققت فيها نتيجتها أو كان يراد أن تتحقق فيها".

ولما كان ذلك، وكان الثابت من الأوراق أن الواقعة محل الاتهام تم نشرها بموقع إيلاف على شبكة الإنترنت، وأن المجني عليها حين اطلاعها على الموقع أثناء وجودها بدبي طالعت الخبر محل الاتهام، ومن ثم تكون نتيجة الفعل قد تحققت في إمارة دبي، وتُعتبر الجريمة إذا ما استوفت باقي أركانها قد وقعت في إقليم الدولة، وتخضع لأحكام قانون العقوبات الاتحادي رقم (3) لسنة 1987، ومن ثم تقضي المحكمة بإلغاء الحكم المستأنف باختصاص محكمة دبي الابتدائية.

وحكمت محكمة الاستئناف بإلغاء الحكم وباختصاص المحكمة، وعلى النيابة العامة إعلان الغائبين من الخصوم بذلك[72].

كما نصت المادة (23) من قانون العقوبات الاتحادي على "لا تقام الدعوى الجنائية على مرتكب جريمة في الخارج إلا من النائب العام. ولا يجوز إقامتها على من يثبت أن المحاكم الأجنبية أصدرت حكماً نهائياً ببراءته أو إدانته واستوفى العقوبة، أو كانت الدعوى الجنائية أو العقوبة المحكوم بها سقطت عنه قانوناً، أو حفظت السلطات المختصة بتلك الدولة التحقيق. ويرجع في تقدير نهائية الحكم وسقوط الدعوى أو العقوبة أو حفظ التحقيق إلى قانون البلد الذي صدر فيه الحكم. فإذا كانت العقوبة المحكوم

(72) حكم محكمة استئناف دبي رقم 2003/1248، جزائي.

بها لم تنفذ كاملة وجب استيفاء مدتها. أما إذا كان الحكم بالبراءة صادراً في جريمة مما نُص عليه في المادتين (20 و21)، وكان مبنياً على أن قانون ذلك البلد لا يعاقب عليها، جازت إقامة الدعوى الجنائية عليه أمام محاكم الدولة، وتكون المحكمة الكائنة بمقر عاصمة الاتحاد هي المختصة بنظر الدعوى.

ويشير الباحث إلى أن المادة نصت على أنه إذا وقعت جريمة في الخارج من الجرائم التي تسري عليها أحكام القانون الوطني، تُرفع على مرتكبها الدعوى أمام المحاكم الجزائية في العاصمة وفق المادة (144) من قانون الإجراءات الجزائية، والتي نصت على "إذا وقعت في الخارج جريمة من الجرائم التي تسري عليها أحكام القانون الوطني تُرفع على مرتكبها الدعوى أمام المحاكم الجزائية في العاصمة"، بينما في حال الجرائم الماسة بأمن الدولة عبر استخدام تقنية المعلومات وحين تطبيقها، فلا يمكن الأخذ بالمادة (144) من قانون الإجراءات الجزائية، وذلك للتعارض في تطبيق القانون، وأن الأصح أن يتم التطبيق وفق القرار الوزاري رقم (220) لسنة 2017 بإنشاء النيابة الاتحادية لجرائم تقنية المعلومات، ومقرها في العاصمة أبوظبي.

المطلب الثاني

أنواع الجرائم الإلكترونية الماسة بأمن الدولة الخارجي

يتناول هذا المطلب الجرائم التي نص عليها المرسوم بقانون رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، وخاصة المادة (44)، والتي تندرج تحت الجرائم الماسة بأمن الدولة ومصالحها، والجرائم التي تخدم الجماعات الإرهابية أو الجمعيات أو الهيئات غير المشروعة، وكذلك الجرائم المتعلقة بتقديم معلومات مضللة لمنظمات أو مؤسسات من شأنها الإضرار بمصالح الدولة أو الإساءة لسمعتها أو هيبتها.

وقد تم تقسيم هذا المطلب لفرعين، تم فيهما تناول الجرائم التي تمس أمن الدولة الخارجي، والتي نص عليها قانون مكافحة جرائم تقنية المعلومات، وذلك على النحو التالي:

- **الفرع الأول: الجرائم المتعلقة بالجماعات الإرهابية أو الهيئات غير المشروعة.**
- **الفرع الثاني: الجرائم المتعلقة بتقديم معلومات عير صحيحة أو غير دقيقة من شأنها الإضرار بمصالح الدولة.**

الفرع الأول

الجرائم المتعلقة بالجماعات الإرهابية أو الهيئات غير المشروعة

تستغل الجماعات والمنظمات والجمعيات الإرهابية والهيئات غير المشروعة وسائل تقنية المعلومات ووسائل التواصل الاجتماعي لتسهيل التواصل بين قادتها وأعضائها، وجذب أعضاء جدد للانضمام إليها، كما أنها تستخدم وسائل التواصل الاجتماعي لجمع المعلومات عن أخبار الدول بهدف دراسة أحوال الشعوب، والوقوف على إشكاليات معينة، ومن ثم تغذية هذه الشعوب بمعلومات مضللة، بهدف إثارتها ضد حكوماتهم تدريجياً إلى حين الوصول إلى الانضمام أو الولاء لها، وذلك لما تمتاز به تقنيات المعلومات ووسائل التواصل الاجتماعي من ميزات وخصائص كبيرة كسرعة نقل المعلومة، وإمكانية القيادة والتوجيه عن بعد، وسهولة التخفي، واستعمال الأسماء الرمزية، وسرعة إنشاء حسابات مستخدمة بديلة في حال توقف عمل سابقتها، وتوفير التراسل الخاص، بالإضافة لإمكانية تغذية مصادر الدخل لهذه الجهات من خلال التحايل وخداع المستخدمين، علاوة على سهولة الترويج لأفكار هذه الجهات وإيصالها لأكبر عدد من المتلقين على مستوى العالم، وأخيراً توفر هذه الجهات تقنية التعليم عن بعد لكيفية صناعة وسائل التفجير والتدمير اليدوية، وكيفية استخدامها.[73]

وقد جَرّم المشرع الاتحادي إنشاء أو إدارة أو الإشراف على موقع إلكتروني بما فيها وسائل التواصل الاجتماعي أو نشر معلومات بقصد تسهيل الاتصال بين قيادات أو أعضاء أو استقطاب أعضاء جدد للجماعات إرهابية، أو أي مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة، أو للترويج أو التحبيذ لأفكارها، أو تمويل أنشطتها، أو توفير المساعدة الفعلية لها، كما جَرّم نشر أساليب تصنيع الأجهزة

(73) وجيه الدسوقي المرسي، الأساليب الإلكترونية الحديثة التي تستخدمها التنظيمات الإرهابية في الجرائم الإرهابية، ندوة دور مؤسسات المجتمع المدني في التصدي للإرهاب، جامعة نايف العربية للعلوم الأمنية 2016/08/26، ص 151.

الحارقة أو المتفجرات أو أي أدوات أخرى تستخدم في الأعمال الإرهابية، أو إعادة بث أو نشر أياً مما سبق، أو نشر محتوى يتضمن التحريض على الكراهية بأي وسيلة كانت بما فيها وسائل التواصل الاجتماعي[74]، حيث نصت المادة (26)[75] من المرسوم بقانون اتحادي في شأن مكافحة جرائم تقنية المعلومات على "يعاقب بالسجن مدة لا تقل عن عشر سنوات ولا تزيد على خمسة وعشرين سنة والغرامة التي لا تقل عن مليوني درهم ولا تجاوز أربعة ملايين درهم كل من أنشأ أو أدار موقعاً إلكترونياً أو أشرف عليه أو نشر معلومات على الشبكة المعلوماتية أو وسيلة تقنية معلومات وذلك لجماعة إرهابية أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة بقصد تسهيل الاتصال بقياداتها أو أعضائها، أو لاستقطاب عضوية لها أو ترويج أو تحبيذ أفكارها، أو تمويل أنشطتها، أو توفير المساعدة الفعلية لها، أو بقصد نشر أساليب تصنيع الأجهزة الحارقة أو المتفجرات، أو أي أدوات أخرى تستخدم في الأعمال الإرهابية"[76]، وتكون العقوبة الحبس مدة لا تزيد على خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز مليون درهم لمن حمل محتوى أياً من المواقع المشار إليها في الفقرة الأولى من هذه المادة أو أعاد بثها أو نشرها بأي وسيلة كانت أو تكرر دخوله إليها لمشاهدتها، أو نشر أي محتوى يتضمن التحريض على الكراهية. وللمحكمة – في غير حالات العود – بد من الحكم بالعقوبة المشار إليها في الفقرة السابقة أن تحكم بإيداع المتهم إحدى دور المناصحة أو الحكم بوضعه تحت

(74) حوراء موسى، الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، المرجع السابق، ص 344.

(75) هذه المادة معدلة بموجب المرسوم بقانون اتحادي رقم (2) لسنة 2018م في شأن تعديل بعض مواد المرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(76) نصت المادة (34) من قانون مكافحة الجرائم الإرهابية الاتحادي على "يعاقب بالسجن المؤقت الذي لا تزيد مدته على عشر سنوات كل من روج أو حبذ بالقول أو الكتابة أو بأي طريقة أخرى لأي تنظيم إرهابي أو شخص إرهابي أو جريمة إرهابية مع علمه بذلك".

المراقبة الإلكترونية، ومنعه من استخدام أية من وسائل تقنية المعلومات خلال فترة تقدرها المحكمة، على ألا تتجاوز الحد الأقصى للعقوبة المقررة.[77]

السلوك الإجرامي:

هنا في هذا الجريمة له صورتين، الصورة الأولى هي إنشاء أو إدارة موقع إلكتروني أو الإشراف عليه لجماعة إرهابية أو أي مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة، ويمكن تسمية ذلك بالتنظيمات أو الكيانات الإرهابية، والصورة الثانية هي نشر معلومات لجماعة إرهابية أو أي مجموعة أو منظمة أو هيئة غير مشروعة.

ويُلاحظ من خلال الصورة الأولى أن نص المادة لم يُجَرِم مجرد إنشاء موقع إلكتروني أو إدارته أو الإشراف عليه، وإنما المُجَرَم هو مساعدة تلك للكيانات الإرهابية أو الكيانات غير المشروعة بمختلف مسمياتها جمعية أو منظمة أو هيئة غير مشروعة. كذلك لم يُجَرِم مجرد نشر معلومات، وإنما التجريم هو نشر معلومات لجماعة إرهابية أو أي مجموعة أو جمعية بحسب ما نصت عليه المادة.

أما الصورة الثانية وهي نشر معلومات لجماعة إرهابية، وذلك من خلال استخدام الجماعات الإرهابية أو الكيانات غير المشروعة للشبكة المعلوماتية أو وسائل تقنية المعلومات أو سائل التواصل الاجتماعي في نشر وإذاعة المعلومات التي تتعلق بالإرهاب، وإذاعة معلومات عن صناعة المتفجرات والأسلحة والقنابل أو تجنيد واستقطاب الأفراد ...إلخ.[78]

ولا يلزم لكي يقع النشاط الإجرامي الوارد في هذه المادة أن يأتي الجاني بجميع صور التجريم، وإنما يكفي أن يرتكب إحداها، وبالنسبة للصورة الثانية فيلزم نشر هذه المعلومات على الشبكة المعلوماتية أو

---

(77) تم تعديل أحكام المادة (26) من المرسوم بقانون اتحادي في شأن مكافحة جرائم تقنية المعلومات وفقا لأحكام المرسوم بقانون اتحادي رقم 2 لسنة 2018.

(78) عبدالرزاق الموافي عبد اللطيف، شرح قانون مكافحة تقنية المعلومات، المرجع السابق، ص 62.

إحدى وسائل تقنية المعلومات لنشر المعلومات الإرهابية، كما لا يلزم لقيام المسئولية وقوع جريمة إرهابية، حيث ينصب التجريم على إنشاء الموقع أو الإدارة أو الإشراف عليه، أو نشر المعلومات المتعلقة بتلك الكيانات.[79]

الركن المعنوي:

جريمة إنشاء موقع أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لجماعة إرهابية هي جريمة عمدية، الركن المعنوي فيها يأخذ صورة القصد الجنائي الذي يقوم على عنصر العلم والإرادة، فيجب أن يعلم الجاني بأنه ينشئ موقعاً أو يديره أو يشرف عليه، أو ينشر لكيان إرهابي أو غير مشروع، وسواءً كان منتمياً إليه أم غير ذلك، فإذا كان وقت مباشرة السلوك يجهل أن الموقع لكيان إرهابي أو غير مشروع أو لنشر معلومات عنه الحالة ينتفي القصد الجنائي، ومثال انتفاء العلم أن ينشئ المتهم موقعاً على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لغرض علمي، وبعد ذلك يدخله أحد أعضاء تلك الكيانات، ويخصص الموقع لها أو لنشر معلومات تتعلق بها، وبذلك يجب أن تعمد إرادة الجاني لتسهيل الاتصال بقيادات الكيانات غير المشروعة، أو ترويج أو تحبيذ تمويل أنشطتها، أو توفير المساعدة الفعلية لها، أو نشر أساليب تصنيع الأسلحة أو المتفجرات، أو أي أدوات أخرى تستخدم الأعمال الإرهابية.

(79) عبدالرزاق الموافي عبد اللطيف، شرح قانون مكافحة تقنية المعلومات، المرجع السابق، ص 64.

العقوبات المقررة للجريمة:

نص المرسوم على معاقبة الجاني بالسجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن مليون درهم ولا تجاوز مليوني درهم. ويُلاحظ أن المرسوم قرر عقوبة السجن ووضع حد أدنى لها وهو خمس سنوات، وفي هذا اتجاه نحو التشديد.

ويؤيد الباحث التشديد في هذا السلوك الإجرامي، وذلك نظراً لخطورة هذه الجماعات وما تقوم به من أفعال؛ حيث كانت العقوبة في القانون القديم هي الحبس مدة لا تزيد على خمس سنوات، وترك الحد الأقصى للسجن للقواعد العامة، والذي لا يزيد عن خمس عشرة سنة، بينما القانون الجديد جعل الجريمة جناية، وأضاف المرسوم الجديد بقانون عقوبة الغرامة التي لا تقل عن مليون درهم ولا تجاوز مليوني درهم، وهي لم تكن موجودة في القانون القديم، كما جعل الجمع بين السجن والغرامة وجوبي، حيث يجب على القاضي النطق بهما معا وإلا كان الحكم معيباً.

الفرع الثاني

الجرائم المتعلقة بتقديم معلومات عير صحيحة أو غير دقيقة من شأنها الإضرار بمصالح الدولة

تتشابه هذه الجريمة بشكل كبير بجريمة السعي أو التخابر مع دولة أجنبية ضد الدولة، وهي جريمة من شأنها الإضرار بمركز الدولة الحربي أو السياسي أو الاقتصادي، اذ يُعرف السعي أو التخابر بأنه أي سلوك مادي ذو مضمون نفسي يتمثل في الاتصال بالدولة الأجنبية أو بأحد العاملين لمصلحتها بقصد إثارة عداوته للوطن[80]، وجريمة السعي أو التخابر لدى دولة أجنبية هي جريمة شكلية، ركنها المادي ارتكاب فعل السعي أو التخابر، ولو لم يتحقق الغرض أو النتيجة التي يهدف إليها الجاني، ولا يشترط الإضرار بمركز الدولة الحربي أو السياسي أو الاقتصادي، ويكفي أن يكون من شأن السعي أو التخابر إحداث هذا الأثر[81].

وقد نصت المادة (38) من المرسوم بقانون اتحادي في شأن مكافحة جرائم تقنية المعلومات على "يعاقب بالسجن المؤقت كل من قدم إلى أي منظمات أو مؤسسات أو هيئات أو أي كيانات أخرى معلومات غير صحيحة أو غير دقيقة أو مضللة، وكان من شأنها الإضرار بمصالح الدولة أو الإساءة إلى سمعتها أو هيبتها أو مكانتها وذلك باستخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات".

السلوك الإجرامي:

(80) حوراء موسى، الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، المرجع السابق، ص 352.

(81) انظر شبكة المحامين العرب.

https://www.mohamoon-ju.com/Default.aspx?action=QAAllJP&FIID=1453&Court=344

محل السلوك الإجرامي هنا هو المعلومات، ويقصد بها البيانات التي تمت معالجتها بحيث أصبحت ذات معنى وصارت مرتبطة بسياق معين، ومثال ذلك المعلومات السياسية، وهي المرتبطة بسياق سياسي، والمعلومات الاقتصادية وهي المرتبطة بسياق اقتصادي، كما يُقصد بالمعلومات غير الصحيحة تلك المعلومات غير المطابقة للواقع، ويُقصد بالمعلومات غير الدقيقة تلك المعلومات المنقوصة غير الكاملة، ويُقصد بالمعلومات المضللة تلك المعلومات الكاذبة والخادعة.

ويتحقق السلوك بقيام الجاني بتقديم معلومات معينة، ويتحقق هذا السلوك سواءً أعطى الجاني المعلومات بناءً على طلب منه أو أعطاها دون أن تُطلب منه، ولم يشترط القانون صفة معينة في الفاعل، فقد يكون موظفاً أو غير ذلك، وتقع الجريمة سواءً تم إعطاء المعلومات لمنظمات أو مؤسسات أو أي كيانات.

والإضرار بمصالح الدولة له العديد من الأوجه سواءً الاقتصادية أو العسكرية أو الثقافية ...إلخ، لكن أهم المصالح هي أمن الدولة وبقائها، والسعي وراء الثروة والنمو الاقتصادي والقوة، ويتجسد الإضرار بمصالح الدولة في إصابتها باذئ أو خسارة، والإضرار قد يهدد كيان الدولة الخارجي أو استقرارها السياسي أو الثقافة العامة، أو مؤسساتها ونظمها الإدارية أو الاقتصادية، ولا تقع هذه الجريمة إذا أضرت بمصالح الغير دون الدولة، كما تقع الجريمة ولو لم يترتب عليها أي نفع شخص للجاني[82].

ويجب أن تتجه إرادة الجاني الى تقديم تلك المعلومات التي يقوم عليها السلوك الإجرامي الوارد في المادة (38) من القانون، وينتفي الركن المعنوي حال انتفاء العلم أو الإرادة أو الإثنين معا، وبالتالي لا تقع الجريمة.

(82) عبدالرزاق الموافي عبد اللطيف، شرح قانون مكافحة تقنية المعلومات، المرجع السابق، ص 129.

ويستدل على ذلك من عبارات نص المادة (38) من القانون، والتي لم تستلزم العمد صراحة، وهذا يؤدي إلى تطبيق المادة (43) من قانون العقوبات الإماراتي، والتي تنص على أنه يسأل الجاني عن الجريمة سواءً ارتكبها عمداً أم خطأً، ما لم يشترط القانون العمد صراحة.

العقوبات المقررة للجريمة:

استحدثت المادة (38) جريمة تقديم معلومات غير صحيحة أو غير دقيقة أو مضللة من شأنها الإضرار بمصالح الدولة، أو الإساءة إلى سمعتها أو هيبتها أو مكانتها، وذلك من خلال استخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.

وقد نص المشرع على عقوبة وحيدة لهذه الجريمة وهي السجن المؤقت، وبالتالي ليس أمام القاضي إلا الحكم بها في حالة الإدانة، فهو لا يتمتع بسلطة تقديرية بشأنها، ولكنه يتمتع بسلطة تقديرية بالنسبة لمدتها، فالحد الأدنى لها ثلاث سنوات، والحد الأقصى خمس عشرة سنة، وذلك وفقا للقواعد العامة.[83]

ويتضح من نوعية العقوبة المنصوص عليها لهذه الجريمة أنها جناية؛ حيث خصص لها المشرع عقوبة السجن، والتي تندرج تحت الجنايات.

وتحكم المحكمة بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب هذه الجريمة أو الأموال المتحصلة منها، وبمحو وإعدام البيانات أو المعلومات، كما تحكم المحكمة بإغلاق المحل أو الموقع الذي أُرتكبت فيه الجريمة، وذلك إغلاقاً كلياً أو المدة التي تقدرها المحكمة.

وتقضي المحكمة أيضاً بإبعاد الأجنبي الذي يُحكم عليه بالإدانة، وهي عقوبة نص عليها هذا المرسوم بقانون، وذلك بعد تنفيذ العقوبة الأصلية، كذلك أجاز المشرع للمحكمة أن تأمر بوضع المحكوم عليه تحت الإشراف أو المراقبة، أو حرمانه من استخدام أي شبكة معلوماتية، أو نظم المعلومات

(83)عبدالرزاق الموافي عبد اللطيف، شرح قانون مكافحة تقنية المعلومات، المرجع السابق، ص 130.

الإلكترونية، أو أي وسيلة تقنية معلومات أخرى، أو وضعه في مأوى علاجي أو مركز تأهيل للمدة التي تراها المحكمة مناسبة، وهو ما سوف يتم تفصيله في الفصل الثاني.

الفصل الثاني

السياسة العقابية لمواجهة الجرائم الإلكترونية الماسة بأمن الدولة ومصالحها

تكمن أهمية السياسة العقابية في مكافحة الجريمة الإلكترونية على مدى خطورة الجرائم الإلكترونية عبر الشبكة المعلوماتية وتزايدها، والآثار السلبية الخطيرة التي تنتجها، وأثرها على المجتمع والدولة، ومما يزيد من أهمية هذه الدراسة الانتشار المتزايد لشبكة تقنية المعلومات عبر وسائل التواصل الاجتماعي، والشبكات التقنية والهواتف الذكية والأجهزة الإلكترونية الأخرى، والتي أصبحت متاحة للجميع بجودة عالية وأسعار تنافسية، وهو ما أدى لزيادة أعداد الجرائم التي باتت تهدد شبكات تقنية المعلومات، لهذا تتمثل الأهمية في التعرف على بيان أهم التحديات التي قد تواجها جهود مكافحة الجرائم الإلكترونية.

وتسعى الدول لحماية نفسها من الجريمة بوسائل متعددة، وبشكل يكفل لها الاستقرار والأمان، وإزاحة كل ما من شأنه أن يعكر صفو الحياة الهانئة الهادئة المستقرة لمجتمعاتهم، وذلك عن طريق سن القوانين والتشريعات، وضمان العدالة الجنائية، وردع التصرفات التي تنال من النظام الاجتماعي لتلك الدول عن طريق الجزاء الجنائي، فالعقوبة بمفهومها لم تكن أمراً جديداً يطرأ على حياة الإنسان، بل إنها تُعد من أبرز مظاهر سيادة الدولة في المجتمع الحديث.

وقد تم تقسيم هذا الفصل لمبحثين تم فيهما تناول نطاق الاختصاص القضائي، والعقوبات والسياسة العقابية لمواجهة الجرائم الإلكترونية الماسة بأمن الدولة ومصالحها، وذلك على النحو التالي:

- **المبحث الأول: نطاق الاختصاص القضائي بنظر الجرائم الإلكترونية الماسة بأمن الدولة.**
- **المبحث الثاني: العقوبات والتدابير الاحترازية لمواجهة الجرائم الماسة بأمن الدولة ومصالحها.**

المبحث الأول

نطاق الاختصاص القضائي بنظر الجرائم الإلكترونية الماسة بأمن الدولة

تُعد جرائم تقنية المعلومات بما فيها الجرائم المرتكبة عبر وسائل التواصل الاجتماعي من أكثر الجرائم المثيرة لإشكالية الاختصاص القضائي، ولكن تنتفي هذه الإشكالية متى كانت الجريمة مرتكبة في إقليم ذات الدولة، إذ ينعقد الاختصاص للمحاكم الوطنية المحلية وفقاً لما تحدده القواعد العامة الواردة في قانون العقوبات الاتحادي، ولكن تتمحور الإشكالية متى كانت الجريمة عابرة للحدود، خاصة في ظل اختلاف التشريعات التي قد ينجم عنها تنازع في الاختصاص بين الدول بالنسبة لهذا النمط من الجرائم، وذلك لأن طبيعة تلك الجرائم المرتكبة عبر شبكة الإنترنت وهي شبكة دولية، من شأنها أن تؤدي إلى أن يصبح إقليم أكثر من دولة محلاً لارتكاب ذات الجريمة.[84]

ولم يخرج المشرع بشأن الجرائم المرتكبة بواسطة شبكة الإنترنت بما فيها الجرائم المرتكبة عبر وسائل التواصل الاجتماعي على القواعد العامة في الاختصاص القضائي بنظر الجريمة، أي أنه لم يخصص لها أحكاماً خاصة تتعلق بالاختصاص القضائي، نظراً لصعوبة ذلك ولاعتبارات ترجع إلى لطبيعة هذه الجرائم، ما يجعل من القواعد العامة المنصوص عليها في قانون العقوبات الاتحادي واجبة التطبيق بمراعاة طبيعة تلك الجرائم.[85]

ويُعتبر قانون العقوبات أكثر القوانين التصاقاً بسيادة الدولة، فهو يطبق بسلطتها لأجل توفير وتأمين الحماية لها ولكافة الأفراد الذين يعيشون على إقليمها وتحت سيادتها، لذا فإن الدولة هي التي تملك سلطة العقاب تجاه كل من ينتهك نصوص التجريم والعقاب في حدود إقليمها.

---

(84) حوراء موسى، الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، المرجع السابق، ص 953.

(85) حوراء موسى، الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، المرجع السابق، ص 954 – 955.

ونظراً لارتباط التجريم والعقاب بسيادة الدولة، فإن ذلك يجعل نطاق تطبيق قانون العقوبات مرتبطاً بمحورين، المحور الأول يعبر عنه بالشق الإيجابي بتطبيق نصوص التجريم والعقاب النافذة على الجرائم المرتكبة في النطاق المكاني لكافة عناصر الإقليم الخاضع لسيادة الدولة، والمحور الثاني يعبر عنه بالشق السلبي، ويعني عدم امتداد قانون العقوبات لملاحقة مرتكبي الجرائم التي تتم خارج الإقليم الخاضع لسيادة الدولة.[86]

وإذا كان تطبيق قانون العقوبات من حيث المكان يدور في فلك هذين المحورين، إلا أن هناك اعتبارات معينة قد أدت إلى الخروج عليهما، فقد أصبح في الإمكان سريان القانون الوطني على جرائم ترتكب خارج إقليم الدولة لحماية مصلحتها، وأصبح في الإمكان كذلك عدم تطبيق القانون الوطني على بعض الجناة الذين يرتكبون جرائمهم على الإقليم الوطني؛ بسبب عدم خضوعهم للقضاء الوطني لاعتبارات قد تكون داخلية أو دولية.[87]

وتنص المادة (16) من قانون العقوبات على أن "تسري أحكام هذا القانون على كل من يرتكب جريمة في إقليم الدولة. ويشمل إقليم الدولة أراضيها وكل مكان يخضع لسيادتها بما في ذلك المياه الإقليمية والفضاء الجوي الذي يعلوها. وتُعتبر الجريمة مرتكبة في إقليم الدولة إذا وقع فيها فعل من الأفعال المكونة لها أو إذا تحققت فيها نتيجتها أو كان يراد أن تتحقق فيها"[88]، وقد نص المشرع

---

(86) غنام محمد غنام، فتيحة محمد قوراري، المبادئ العامة في قانون الإجراءات الجزائية لدولة الإمارات العربية المتحدة، دار الآفاق المشرقة، الشارقة، 2011، ص 260.

(87) غنام محمد غنام، فتيحة محمد قوراري، المبادئ العامة في قانون الإجراءات الجزائية لدولة الإمارات العربية المتحدة، المرجع السابق، ص 263.

(88) المادة (16) من القانون الاتحادي رقم (3) لسنة 1987 وفقاً لأحدث التعديلات الواردة بالمرسوم بقانون رقم (7) لسنة 2016م.

المصري أيضاً على ذلك في قانون العقوبات، إذ نصت المادة (1) على "تسري أحكام هذا القانون على كل من يرتكب في القطر المصري جريمة من الجرائم المنصوص عليها فيه".[89]

كما نصت المادة (47) من قانون مكافحة جرائم تقية المعلومات الإماراتي على "مع عدم الإخلال بأحكام الفصل الثاني من الباب الثاني من الكتاب الأول من قانون العقوبات، تسري أحكام هذا المرسوم بقانون على كل من ارتكب إحدى الجرائم الواردة به خارج الدولة إذا كان محلها نظام معلوماتي إلكتروني أو شبكة معلوماتية أو موقع إلكتروني أو وسيلة تقنية معلومات خاصة بالحكومة الاتحادية أو إحدى الحكومات المحلية لإمارات الدولة أو إحدى الهيئات أو المؤسسات العامة المملوكة لأي منهما".[90]

كما حددت المادة (47) نطاق تطبيق أحكام المرسوم الجديد بقانون، حيث قررت تطبيق أحكامه على كل شخص يرتكب جريمة من الجرائم المنصوص عليها فيه خارج الدولة إذا كان محلها نظام معلوماتي إلكتروني أو شبكة معلوماتية أو موقع إلكتروني أو وسيلة تقنية معلومات تخص الحكومة الاتحادية أو إحدى الحكومات المحلية لإمارات الدولة، أو تخص إحدى الهيئات أو المؤسسات العامة المملوكة للحكومة الاتحادية أو إحدى الحكومات المحلية لإمارات الدولة.

وذلك دون الإخلال بأحكام قانون العقوبات الاتحادي لدولة الإمارات المتعلقة بسريانه من حيث المكان والأشخاص، وبالتالي تضاف هذه الجرائم إلى طائفة الجرائم المنصوص عليها في المادة (20) من قانون العقوبات[91].

---

(89) المادة (1) من قانون العقوبات المصري رقم 58 لسنة 1937 والتعديل عليه بالقانون رقم 189 لسنة 2020.

(90) المادة (47) من القانون الاتحادي رقم 2 لسنة 2018 في شأن قانون مكافحة جرائم تقية المعلومات.

(91) نصت المادة (20) على "يسري هذا القانون على كل من ارتكب فعلاً خارج الدولة يجعله فاعلاً أو شريكاً في جريمة من الجرائم الآتية: 1 – جريمة ماسة بأمن الدولة الخارجي أو الداخلي أو ضد نظامها الدستوري أو سنداتها المالية المأذون بإصدارها قانوناً أو طوابعها أو جريمة تزوير أو تقليد محرراتها أو أختامها الرسمية. 2 – جريمة تزوير أو تقليد أو تزييف عملة الدولة أو ترويجها أو حيازتها بقصد ترويجها سواءً تمت تلك الأفعال داخل الدولة أو خارجها. 3 –

ويرى الباحث أن هذا ليس استثناءً على خلاف المادة (20) من قانون العقوبات الاتحادي، وإنما استثناءً أضاف إليها جرائم أخرى بوصف المادة (47)، وهي الجرائم المنصوص عليها فيه خارج الدولة إذا كان محلها نظام معلوماتي إلكتروني أو شبكة معلوماتية أو موقع إلكتروني أو وسيلة تقنية معلومات تخص الحكومة الاتحادية أو الحكومات المحلية لإمارات الدولة، أو تخص إحدى الهيئات أو المؤسسات العامة سواءً اتحادية أو محلية.

وفيما يتعلق الاختصاص القضائي لنظر الجرائم الماسة بأمن الدولة، فلم يورد المشرع الاتحادي تعريفاً محدداً للجرائم التي تمس أمن الدولة ومصالحها، وترك ذلك للفقه والقضاء، كون أن دستور الدولة وقانون المحكمة الاتحادية العليا عرفها تعريفاً ضمنياً بأنها تلك الجرائم التي لها مساس مباشر بمصالح الاتحاد، ومن ثم جاءت القوانين الاتحادية من هذا التعريف بتفسير بعض الأفعال التي تمس مصالح الدولة مثل الجرائم المتعلقة بأمن الدولة في الداخل والخارج، والجرائم التي تدخل في تزوير المحررات والأختام الرسمية لمؤسسات الدولة الاتحادية، وجرائم تزييف العملات، وجرائم الإرهاب وتفرعاتها ...وغيرها.[92]

وعندما يأتي تطبيق القانون على الجرائم الماسة بأمن الدولة في الداخل أو الخارج، يتم نظرها من قِبل الدائرة الجزائية في محكمة أبوظبي الاتحادية الاستئنافية، مع إمكان الطعن في أحكام محكمة الاستئناف أمام المحكمة الاتحادية العليا، والتي تكون أحكامها نهائية وملزمة وفق القانون الاتحادي رقم

جريمة تزوير أو تقليد أو تزييف عملة ورقية أو مسكوكات معدنية متداولة قانوناً في الدولة أو ترويج تلك العملات والمسكوكات فيها أو حيازتها بقصد ترويجها".

(92) عبد الوهاب عبدول، المختصر في جرائم أمن الدولة والمحكمة المختصة بنظرها، صفحة بن نخيره ومشاركوه، تاريخ الزيارة 2018/10/16.

https://www.lianapress.ae/releases/finance/d8-a7-d9-84-d9-85-d8-ae-d8-aa-d8-b5-d8-b1-d9-81-d9-8a-d8-ac-d8-b1-d8-a7-d8-a6-d9-85-d8-a7-d9-85-d9-86-d8-a7-d9-84-d8-af-d9-88-d9-84-d8-a9-d9-88-d8-a7-d9-84-d9-85-d8-ad-d9-83-d9-85-d8-a9-d8-a7-d9-84-d9-85-d8-ae-d8-aa-d8-b5-d8-a9-d8-a8-d9-86-d8-b8-d8-b1-d9-87-d8-a7.html

11 لسنة 2016[93]، حيث نصت المادة (2) من المرسوم بقانون اتحادي على أن تضاف مادة جديدة برقم 12 مكرر للقانون الاتحادي رقم 3 لسنة 1983، والتي نصت على "تختص الدائرة الجزائية في محكمة أبوظبي الاتحادية الاستئنافية دون غيرها بالفصل في الدعاوى المتعلقة بالجرائم التي لها مساس مباشر بمصالح الاتحاد كالجرائم المتعلقة بأمنه في الداخل والخارج، وجرائم تزوير المحررات أو الأختام الرسمية لإحدى السلطات الاتحادية، وجرائم تزوير العملة، ويُطعن في الأحكام الصادرة منها أمام المحكمة الاتحادية العليا التي تكون أحكامها نهائية وملزمة للكافة".[94]

وتمثل النيابة العامة أمام هذه الدائرة بنيابة متخصصة تسمي (نيابة جرائم تقنية المعلومات)، وتتولي الادعاء باسم المجتمع، وتتبع هذه النيابة النائب العام الاتحادي[95]، وقد نصت المادة (2) من القرار الوزاري رقم 220 لسنة 2017 بشأن إنشاء نيابة جرائم تقنية المعلومات على "تختص النيابة الاتحادية لجرائم تقنية المعلومات بالتحقيق والتصرف ومباشرة الدعاوى الجزائية في الجرائم المنصوص عليها في المواد (17، 19، 23، 25، 27، 31، 32، 35، 36، 37) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات والجرائم المرتبطة بها ارتباطاً لا يقبل التجزئة، والتي تقع في دوائر الاختصاص المكاني للنيابات العامة الاتحادية".[96]

كما نصت المادة (3) من القرار الوزاري رقم 220 لسنة 2017 بشأن إنشاء نيابة جرائم تقنية المعلومات على "للنائب العام – ووفقاً لما يقدره تحقيقاً لاعتبارات مصلحة العمل – إحالة بعض الجرائم

(93) القانون الاتحادي رقم 3 لسنة 1983 بشأن السلطة القضائية الاتحادية.

(94) المادة (2) من المرسوم بقانون اتحادي رقم 3 لسنة 1983 بشأن السلطة القضائية الاتحادية.

(95) القرار الوزاري رقم (220) لسنة 2017 بإنشاء النيابة الاتحادية لجرائم تقنية المعلومات ومقرها في العاصمة أبوظبي.

(96) القرار الوزاري رقم (220) لسنة 2017، صادر بتاريخ 2017/3/12 بشأن إنشاء نيابة جرائم تقنية المعلومات.

الواردة في الفقرة الأولى من المادة الثانية من هذا القرار إلى النيابات الاتحادية لمباشرة التحقيق، وفي جميع الأحوال يكون التصرف من نيابة جرائم تقنية المعلومات".[97]

وتحيل الأجهزة الأمنية كافة تحرياتها واستدلالاتها عن هذه الجرائم إلى نيابة أمن الدولة بغض النظر عن مكان وقوعها، ودون التقيد بقواعد الاختصاص المكاني المنصوص عليها في قانون الإجراءات الجزائية.[98]

ومع التي طرأت على الدولة سياسياً واقتصادياً واجتماعياً وفي كافة المجالات، وهو ما أدى لاختلاف طبيعية الجرائم ومدى تأثيرها على المجتمع، فيقف القضاء الاتحادي كسلطة مستقلة، فالقضاة مستقلون لا سلطان عليهم في أداء واجبهم لغير القانون وضمائرهم.

وقد خصص دستور دولة الإمارات العربية المتحدة الباب الرابع لولاية المحكمة الاتحادية، حيث ينص فيه على استقلال القضاء، كما نظمها القانون الاتحادي رقم 6 لسنة 1978 بشأن المحاكم.

وتختص المحكمة الاتحادية بالنظر في العديد المسائل من مثل "المنازعات المختلفة بين الإمارات الأعضاء في الاتحاد، وبحث دستورية القوانين الاتحادية، وبحث دستورية التشريعات الصادرة والقوانين واللوائح عموماً... وغيرها". [99]

ويأتي ضمان تنظيم القضاء واستقلاله على أسس التنظيم السليم للسلطة القضائية من تحديد أنواع المحاكم ودرجاتها (محاكم ابتدائية، محاكم استئنافية، محاكم عليا) [100] وذلك وفق نص المادة (95)

---

(97) القرار الوزاري رقم (220) لسنة 2017، صادر بتاريخ 2017/3/12 بشأن إنشاء نيابة جرائم تقنية المعلومات.

(98) غنام محمد غنام، فتيحة محمد قوراري، المبادئ العامة في قانون الإجراءات الجزائية لدولة الإمارات العربية المتحدة، المرجع السابق، ص 260.

(99) المادة (99) من الدستور الاتحادي لدولة الإمارات العربية المتحدة لعام 1971 وتعديلاته.

(100) نواف كنعان، النظام الدستوري والسياسي لدولة الإمارات العربية المتحدة، مكتبة الجامعة، الشارقة، الطبعة الثانية، 2006، ص 278.

من الدستور والتي نصت على "يكون للاتحاد محكمة اتحادية عليا، ومحاكم اتحادية ابتدائية وذلك على الوجه المبين في المواد التالية)[101]، كما نصت المادة (103) على "... ويجوز أن ينص القانون على استئناف أحكام تلك المحاكم أمام إحدى دوائر المحكمة الاتحادية العليا في الحالات وبالإجراءات التي يحددها".[102]

ومن خلال اطلاع الباحث على تاريخ المحكمة الاتحادية العليا منذ وضع الدستور وحتى الوقت الحالي، فقد اتضح حدوث تغيرات بالنسبة للمحاكم تحت ولاية المحكمة الاتحادية، وقد نصت المادة (99) من الدستور على "... 6- الجرائم التي لها مساس مباشر بمصالح الاتحاد، كالجرائم المتعلقة بأمنه في الداخل أو الخارج، وجرائم تزوير المحررات أو الأختام الرسمية لإحدى السلطات الاتحادية، وجرائم تزييف العملة...".

وعندما يأتي تطبيق القانون قبل عام 2016، فإن الجرائم الماسة بأمن الدولة في الداخل أو الخارج كان يتم نظرها من قِبل المحكمة الاتحادية العليا، فيما كان المعمول به التقاضي مباشرة أمام دائرة أمن الدولة في المحكمة الاتحادية العليا التي تصدر أحكاماً قطعية غير قابلة للطعن.

ثم صدر قانون اتحادي بشأن التقاضي في القضايا الخاصة بأمن الدولة على مرحلتين، حيث تنظر فيها الدائرة الجزائية في محكمة أبوظبي الاتحادية الاستئنافية، مع إمكان الطعن في أحكام محكمة الاستئناف أمام المحكمة الاتحادية العليا التي تكون أحكامها نهائية وملزمة وفق القانون الاتحادي رقم 11 لسنة 2016 بشأن تعديل بعض أحكام القانون الاتحادي رقم 3 لسنة 1983 بشأن السلطة القضائية الاتحادية، حيث نصت المادة (2) من المرسوم بقانون اتحادي على أن تضاف مادة جديدة برقم 12 مكرر للقانون الاتحادي رقم 3 لسنة 1983 وتنص على "تختص الدائرة الجزائية في محكمة أبوظبي

(101) المادة (95) من الدستور الاتحادي لدولة الإمارات العربية المتحدة لعام 1971 وتعديلاته.
(102) المادة (103) من الدستور الاتحادي لدولة الإمارات العربية المتحدة لعام 1971 وتعديلاته.

الاتحادية الاستئنافية دون غيرها بالفصل في الدعاوى المتعلقة بالجرائم التي لها مساس مباشر بمصالح الاتحاد كالجرائم المتعلقة بأمنه في الداخل والخارج، وجرائم تزوير المحررات أو الأختام الرسمية لإحدى السلطات الاتحادية، وجرائم تزوير العملة، ويُطعن في الأحكام الصادرة منها أمام المحكمة الاتحادية العليا التي تكون أحكامها نهائية وملزمة للكافة".[103]

يأتي ذلك إلى ضمان تحقيق الأسس التي وضعها الدستور لكفالة حق الأفراد وتحقيق النزاهة في التقاضي.

(103) نص المادة (12) مكرر من المرسوم بقانون اتحادي 11 لسنة 2016 بشأن تعديل بعض أحكام القانون الاتحادي رقم (3) لسنة 1983 في شأن السلطة القضائية الاتحادية.

المبحث الثاني

العقوبات والتدابير الاحترازية لمواجهة الجرائم الماسة بأمن الدولة ومصالحها

الأصل أن العقوبات الأصلية المقررة في جرائم أمن الدولة هي العقوبات التي يجوز الحكم بها على الجاني منفردة، فتكفي عن غيرها لمقابلة فعل الجاني، ولذلك تسمى بالعقوبات الأصلية، وتُعرف العقوبة الأصلية بأنها الجزاء الذي حدده المشرع لهذه الجريمة، بحيث لا تقترن بأي عقوبة أخرى، وهي العقوبات التي قررها القانون للجريمة فور وصفه لنموذجها.[104]

وقد عَرّف الدكتور محمد شلال عقوبة الإعدام بأنها إزهاق روح المحكوم عليه الذي صدر ضده حكم من قِبل محكمة متخصصة، لارتكابه جناية خطيرة يعاقب عليها القانون".[105]

ولفظ عقوبة الإعدام هو لفظ جرى تداوله وأصبح معروفاً في عصرنا الحالي ليدل على إزهاق روح المحكوم عليه بهذه العقوبة، واستئصال حياته نهائياً من الوجود من خلال الإجراءات والوسائل المنصوص عليها قانوناً، وذلك بسبب ارتكابه جريمة استحقت هذه العقوبة، وقد عُرفت العقوبة بأنها جزاء يقرره المشرع ويوقعه القاضي على كل من تثبت مسؤوليته عن الجريمة، ويتضمن إيلاماً بهدف ردعه وإصلاحه لمصلحة الهيئة الاجتماعية".[106]

ومنذ القدم، كانت العدالة تقاس على أساس أخذ العقوبة من طبيعة الجريمة الواقعة، وعقوبة الإعدام ترضي الشعور الإنساني في المجتمع بأن المخطئ لا بد وأن يلقى جزاءه، وإذا لم يعطِ المجتمع الحق في الحياة، فإنه كذلك لن يعطِ الحق في الحرية، فكيف له أن يسجن الناس ويمنعهم من الحرية، فمثلما

---

(104) رمسيس بهنام، النظرية العامة للقانون الجنائي، منشاة المعارف، الإسكندرية، 1995، ص 907.

(105) رضا الغزاوي، عقوبة الإعدام في الوطن العربي، المنظمة المصرية للإصلاح الجنائي، القاهرة، 2007، ص 12.

(106) فهد يوسف الكساسبة، وظيفة العقوبة ودورها في الإصلاح والتأهيل، دار وائل، عمّان، 2010، ص 17.

للإنسان الحق في الحياة، فله كذلك الحق في الحرية، والاعتراض على شرعية الإعدام يؤدي إلى الاعتراض على شرعية كل العقوبات التي تسلب الحرية. والحياة دون شك غير قابلة للمس أكثر من أي حق آخر، لكن لكل حقوقنا حد، وهو حق الآخرين، فإذا استلزم من أجل إنقاذ حياة الإنسان النزيه أن يموت المجرم، فكيف يمكن الإعلان عن عدم قابلية الحياة البشرية للمس.[107]

إن أحكام العقوبات التكميلية ليست من الأحكام العامة للعقاب، وإنما هي عقوبات تكمل العقوبات العامة، لأنه يجب النص عليها صراحة في الحكم، وقد حدد المشرع الإماراتي في قانون العقوبات على أن العقوبات الفرعية هي العقوبات التبعية والعقوبات التكميلية، فالعقوبات التبعية كما نصت عليها المادة (73) هي الحرمان من بعض الحقوق والمزايا، ومراقبة الشرطة، وتلحق هذه العقوبات المحكوم عليه بقوة القانون دون حاجة إلى النص في الحكم، وذلك على النحو المبين في هذا الفرع.[108]

- **العقوبة التبعية:**

تُعرف العقوبة التبعية بأنها "عقوبة مرتبطة بالعقوبة الأصلية وتصيب الجاني بناءً على العقوبة الأصلية دون الحاجة للحكم بها أو ذكرها في نص الحكم".[109]

- **العقوبة التكميلية:**

هي التي تصيب الجاني بناءً على الحكم بالعقوبة الأصلية بشرط أن يُحْكَم بالعقوبة التكميلية، وتنقسم العقوبة التكميلية إلى نوعين، الأولى وجوبية بحيث يتعين على القاضي أن ينطق بها، والثانية جوازية بحيث يكون النطق بها متوقفاً على تقدير القاضي.

---

(107) سليمان عبد المنعم، مبادئ علم الجزاء الجنائي، دار الجامعة الجديدة، الإسكندرية، 2002، ص 85.

(108) قانون العقوبات الاتحادي رقم (3) لسنة 1987.

(109) رمسيس بهنام، النظرية العامة للقانون الجنائي، المرجع السابق، ص 907.

وقد نص قانون العقوبات الاتحادي على هذا النوع من العقوبات في المواد (82/80)، حيث نصت المادة (80) على "للمحكمة عند الحكم في جناية بالحبس أن تأمر بحرمان المحكوم عليه من حق أو مزية أو أكثر مما نُص عليه في المادة (75) وذلك لمدة لا تقل عن سنة ولا تزيد على ثلاث سنوات تبدأ من نهاية تنفيذ العقوبة أو انقضائها لأي سبب آخر". ومؤدى هذا النص أن للمحكمة الحق في أن تُلحق بالعقوبة الأصلية عقوبة تكميلية، وهي الحرمان من بعض الحقوق والمزايا، وهي عقوبة جوازية مؤقتة تطبق منفردة بعد انقضاء مدة العقوبة الأصلية، وتترك لتقدير المحكمة.

أما بالنسبة للمصادرة فهي عقوبة تكميلية، وقد نصت المادة (82) من قانون العقوبات الاتحادي على "تحكم المحكمة عند الحكم بالإدانة بمصادرة الأشياء والأموال المضبوطة التي أُستعملت فيها أو كان من شأنها أن تستعمل فيها أو كانت محلاً لها أو التي تحصلت من الجريمة. فإذا تعذر ضبط أيا من تلك الأشياء أو الأموال حكمت المحكمة بغرامة تعادل قيمتها وذلك كله دون الإخلال بحقوق الغير حسن النية.

وتُعتبر عقوبة الحرمان من حق المواطنة في جرائم أمن الدولة وهي الصورة الأولى من العقوبات التبعية أو التكميلية، والتي تعني طرد الشخص ونبذه من الجماعة التي يعيش فيها لعدم ولائه لها، وذلك جزاءً لما ارتكبه من جرم في حقها.

وقد حدد المشرع الإماراتي حالات إسقاط الجنسية في المواد (14) مكرر و(15) مكرر من قانون الجنسية وجوازات السفر، والتي جاءت نصوصها على النحو التالي:

"يترتب على الحكم البات الصادر بإدانة المواطن سواءً كان متمتعاً بالجنسية بحكم القانون أو بالتجنس أو بالتبعية إسقاط أو سحب الجنسية كعقوبة تبعية، وذلك في الجرائم الآتية:

1) إذا أُدين في جريمة من الجرائم الإرهابية المنصوص عليها في قانون مكافحة الجرائم الإرهابية.

2) إذا أُدين في جريمة ماسة بالأمن الخارجي للدولة والمعاقب عليها وفقاً لقانون العقوبات الاتحادي أو غيرها من الجرائم التي تعتبر ماسة بالأمن الخارجي للدولة وفقاً للقوانين النافذة بالدولة.

3) تختص محكمة استئناف أبوظبي الاتحادية بالنظر في الجرائم المنصوص عليها في الفقرتين (1-2) من هذه الفقرة، وتحيل النيابة المختصة إليها هذه الجرائم.

4) يشكل وزير العدل دائرة أو دوائر متخصصة في محكمة استئناف أبوظبي الاتحادية للبت في هذه الجرائم، ويكون حكم المحكمة قابلاً للنقض أمام المحكمة الاتحادية العليا وفقاً للقانون".

ولم يخرج المشرع في المرسوم بقانون عن التقسيم الذي جرى وفقاً للقواعد العامة، فقد ورد في المرسوم بقانون رقم 5 لسنة 2012 مجموعة من التدابير الاحترازية الهامة إلى جوار العقوبة تتناسب مع جرائم تقنية المعلومات، حيث تقوم باستكمال دور العقوبة، ولا تنقضي إلا بزوال الخطورة الإجرامية، على عكس العقوبة التي تتحدد لها مدة معينة، وتنقضي دون أن تترك في الجاني أي أثر.

وقد ظهرت فكرة التدابير الاحترازية كوسيلة أخرى لمواجهة السلوك الإجرامي، حيث إن العقوبة وحدها لم تنجح في تحقيق الغرض منها في التشريعات الحديثة[110]، فالعقوبة تعجز في بعض الحالات عن مواجهة الخطورة الإجرامية للمجرمين المعتادين على الإجرام، فمعاودة ارتكاب السلوك الإجرامي دليل على عدم فعاليتها في تحقيق الردع لهذه الفئة، لأن سبب العودة في ارتكاب الجريمة هو الميل الإجرامي واحتراف الإجرام الذي يشكل النصيب الأكبر من تكوين شخصيته، لذلك يستلزم اتخاذ الإجراءات اللازمة لعلاجه، وهو ما أكد عجز العقوبة عن تحقيقه.[111]

(110) محمد أبو العلا عقيدة، أصول علم العقاب: دراسة تأصيلية للنظام العقابي الإسلامي والأنظمة العقابية المعاصرة مقارنة بالنظام العقابي في دولة الإمارات العربية المتحدة، جامعة الإمارات العربية المتحدة، العين، 1999، ص 49.
(111) محمود نجيب حسني، علم العقاب، دار النهضة العربية، القاهرة، الطبعة الثالثة، 1973، ص 48.

وتُعرف التدابير الاحترازية على أنها "إجراءات تُتَخَذ حيال المجرم بهدف إزالة أسباب الإجرام لديه وتأهيله اجتماعياً".[112]

وطبقاً للقواعد العامة لقانون العقوبات الاتحادي لسنة 1987، فإن المشرع وضع حداً أقصى للتدابير ولم يتركه مفتوحاً، فالمهمة الاساسية للتدابير تتمثل في مواجهة الخطورة الإجرامية الكامنة في شخص المجرم، حتى تقوم بتقويمه، وتكون التدابير لاحقة على ارتكاب الجريمة، بمعنى أنه لا يجوز تطبيقها إلا بعد ارتكاب الجريمة، فارتكاب الجريمة مؤشر على وجود الخطورة الإجرامية، كما أن التدابير لا تخضع لقاعدة عدم الرجعية، وذلك حرصاً على حريات الأفراد بحمايتهم من العقاب عن أفعال قد تكون مباحة، أو الحكم عليهم بعقوبات قد تكون مشددة.[113]

ووفقاً للقواعد العامة الواردة في قانون العقوبات الاتحادي فإن التدابير الجنائية تكون على ثلاثة أنواع (التدابير المقيدة للحرية، التدابير السالبة للحقوق، التدابير المادية)، وقد ورد ذكر تلك التدابير في المواد (109- 132)، والمادة (110) حددت التدابير المقيدة للحرية وهي:

1) حظر ارتياد بعض المحال العامة.
2) منع الإقامة في مكان معين.
3) المراقبة.
4) الخدمة المجتمعية.
5) الإبعاد عن الدولة.

وسيتم تناول التدابير التي أشار إليها المشرع في قانون مكافحة جرائم تقنية المعلومات من خلال المطالب التالية:

---

(112) مأمون سلامة، قانون العقوبات القسم العام، دار الفكر العربي، القاهرة، الطبعة الثالثة، 1990، ص 735.
(113) علي محمود علي حمودة، قانون العقوبات: النظرية العامة للجريمة، المرجع السابق، ص 434 – 438.

المطلب الأول

المصادرة

يُقصد بالمصادرة أخذ أموال من مالكها وإضافتها لأملاك الدولة بدون مقابل، فالدولة تتملك الأشياء قهراً ويغير مقابل، والأصل أن المصادرة عقوبة فرعية تكميلية جوازية، وللمحكمة سلطة تقدير الحكم بها أو غير ذلك، وفي بعض الحالات تكون وجوبية، ويَلْزَم أن ينطق بها القاضي في حكمه.[114]

وقد نصت المادة (82) من قانون العقوبات الاتحادي على المصادرة، وأشار إليها المشرع بأنها عقوبة تكميلية لا توقع إلا بحكم من القاضي، كما أنها عقوبة مشتركة بين جميع الجرائم وفقاً لهذا النص، كما نصت المادة (41) من المرسوم بقانون رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات على هذه العقوبة، ويتضح من المادة (82) من قانون العقوبات أن المصادرة جوازية، وعقوبة تكميلية بالمعنى الدقيق، وفي الحالة الوجوبية تكون تدبيراً وقائياً.[115]

ويكون محل المصادرة كعقوبة هو أثناء حيازتها وتداولها، ويكون مشروعاً في الأصل ومملوكاً للمحكوم عليه، ولكن لاتصالها بالجريمة يتم مصادرتها، كما أن الغرض منها كعقوبة هو إعلام المحكوم عليه وزجره لارتكابه جريمة، ويَلْزَم للحكم بها ضرورة صدور حكم بالإدانة بعقوبة أصلية، ومحلها كتدبير وقائي هو أشياء غير مشروعة، وقد تكون مملوكة للغير، والغرض منها أخذ أشياء خطرة للحيلولة دون استعمالها في ارتكاب الجرائم في المستقبل، وهي كتدبير يحكم بها القاضي حتى ولو صدر قانون بالعفو الشامل أو قضي ببراءة المتهم، وتصبح الأشياء محل المصادرة كعقوبة وتدبير وقائي مملوكة للدولة.[116]

---

(114) حسن محمد ربيع، شرح قانون العقوبات الاتحادي: القسم العام، الجزء الثاني، أكاديمية شرطة دبي، دبي 2005، ص 164.

(115) حسن محمد ربيع، شرح قانون العقوبات الاتحادي: القسم العام، الجزء الثاني، المرجع السابق، ص 147.

(116) عبدالرزاق الموافي عبد اللطيف، شرح قانون مكافحة تقنية المعلومات، المرجع السابق، ص 129.

وبالإضافة إلى العقوبات السابقة، يُحْكَم بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب هذه الجريمة أو الوسائل المتحصلة منها. ويُحْكَم كذلك بإغلاق المحل أو الموقع الذي أُرتكبت فيه الجريمة، سواءً كانت الجريمة قد أُرتكبت بعلم مالكه أم بدون علمه، ويكون الإغلاق كلية أو للمدة التي تقدرها المحكمة، وكذلك تقضي المحكمة بإبعاد الأجنبي الذي يُحْكَم عليه بالحبس وفقاً لأحكام هذا القانون".[117]

(117) محمد عبدالله العوا، الاحتيال عبر الإنترنت وجرائم بطاقات الائتمان، دار النهضة العربية، القاهرة، الطبعة الأولى، 2018، ص 191.

المطلب الثاني

إغلاق المحل أو الموقع الذي ارتكبت فيه الجريمة

نصت المادة (41) من قانون مكافحة جرائم تقنية المعلومات على "مع عدم الإخلال... كما يُحْكَم بإغلاق المحل أو الموقع الذي يُرْتَكَب فيه أي من هذه الجرائم، وذلك إما إغلاقاً كليا أو المدة التي تقدرها المحكمة".

ويُقصد بالغلق الذي تقضي به المحكمة المختصة بحكم قضائي، فهو الغلق الذي يصدر بناءً على حكم بالإدانة صادر من محكمة جنائية، ويقع على المحل أو الموقع الذي أُرتكبت فيه الجريمة، وبالتالي يخرج ذلك المحل أو الموقع من نطاق التعامل متى أُرتكبت السلوكيات التي يجرمها القانون من خلاله.

ومن خلال نص المادة المبينة فقد يكون الغلق كلياً أي بشكل دائم أو بشكل مؤقت، وتخضع مدة الغلق للسلطة التقديرية لقاضي الموضوع، فله التقدير بأن يكون الغلق كلياً، أو يكون له مدة معينة تقدرها المحكمة، ويعني ذلك منع ممارسة السلوك المُجَرَم في الموقع أو المحل للمدة التي تقررها المحكمة، أي استبعاده من الشبكة المعلوماتية.[118]

ولا يشمل الحظر مالك المحل أو الموقع إلا إذا صدر عليه حكم بالإدانة من أجل جريمة من الجرائم المنصوص عليها بالمرسوم رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، حيث يعني الغلق الحيلولة دون تشغيل واستخدام المحل أو الموقع في ارتكاب جرائم تقنية معلومات أخرى، ويستوي أن يكون المحكوم عليه مالكاً أم مستأجراً المحل أو الموقع، ولم يشترط المرسوم للإغلاق أن تكون الجريمة أُرتكبت بعلم المالك؛ حيث كان يشترط ذلك في القانون القديم في المادة (24) منه.[119]

---

(118) محمد عبدالله العوا، الاحتيال عبر الإنترنت وجرائم بطاقات الائتمان، المرجع السابق، ص 191.

(119) المادة (24) من القانون رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات.

ويرى الباحث أن القانون الجديد كان موفقاً عن القانون القديم فيما يتعلق بعملية الإغلاق فيما يتعلق بعلم مالك المحل من عدمه بارتكاب الجريمة، حيث يجب أن يكون التدبير مُلْزِماً في حال كانت الجريمة تقع تحت وصف جرائم أمن الدولة بغض النظر عن أي متغيرات أخرى.

المطلب الثالث

إبعاد الأجنبي

نصت المادة (42) بموجب المرسوم بقانون اتحادي رقم (2) لسنة 2018 على "تقضي المحكمة بإبعاد الأجنبي الذي يُحْكَم عليه بالإدانة لارتكاب أي جريمة من الجرائم المنصوص عليها في هذا المرسوم بقانون وذلك بعد تنفيذ العقوبة المحكوم بها"[120].

ولما كان من المقرر العمل بنص المادة (42) من المرسوم بقانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات والتي تنص على "تقضي المحكمة بإبعاد الأجنبي الذي يُحْكَم عليه بالإدانة لارتكاب أي جريمة من الجرائم المنصوص عليها في هذا المرسوم بقانون وذلك بعد تنفيذ العقوبة المحكوم بها" ويتضح بأن المشرع لم يمنح سلطة تقديرية لقاضي الموضوع في الحكم بإبعاد الأجنبي الذي تثبت إدانته في جريمة من الجرائم المنصوص عليها في هذا المرسوم بقانون، بما معناه وجوب الحكم بهذا التدبير في جميع الأحوال التي يدان فيها الأجنبي بجريمة من الجرائم المنصوص عليها في هذا المرسوم بقانون، وبطبيعة الحال فإن الإبعاد يكون للأجنبي الذي يُحَكَم عليه بالإدانة لارتكاب أي جريمة من الجرائم المنصوص عليها في هذا المرسوم بقانون، وذلك بعد قضاء العقوبة المحكوم بها.[121]

---

(120) هذه المادة معدلة بموجب المرسوم بقانون اتحادي رقم (2) لسنة 2018م في شأن تعديل بعض مواد المرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات "مع مراعاة حكم الفقرة الثانية من المادة (121) من قانون العقوبات، تقضي المحكمة بإبعاد الأجنبي الذي يحكم عليه في أي من الجرائم الواقعة على العرض، أو يحكم عليه بعقوبة الجناية في أي من الجرائم المنصوص عليها في هذا المرسوم بقانون، وذلك بعد تنفيذ العقوبة المحكوم بها".

(121) محمد عبدالله العوا، الاحتيال عبر الإنترنت وجرائم بطاقات الائتمان، المرجع السابق، ص 193.

ويرى الباحث بأن المشرع كان موفقاً بإحلال المادة (42) من المرسوم الجديد محل المادة (25) من القانون القديم والتشديد على الجاني الإبعاد، حيث أوجبت الإبعاد في حالة الحكم بالإدانة في جريمة من الجرائم المنصوص عليها في هذا المرسوم بقانون، سواءً صدر الحكم بعقوبة سالبة للحرية (السجن أو الحبس) أو بعقوبة الغرامة، ووجه التشديد هو أن القانون القديم كان يوجب الإبعاد حالة صدور الحكم بالحبس فقط، وبالتالي كان لا يجوز الإبعاد في حالة الحكم بالغرامة فقط.

كما أن التعديل الذي طرأ على الإبعاد الوجوبي جاء لمراعاة نص المادة (121) من قانون العقوبات، والتي نصت على "إذا حُكِم على أجنبي في جناية بعقوبة مقيدة للحرية وجب الحكم بإبعاده عن الدولة، ويجوز للمحكمة في مواد الجنح الأخرى أن تأمر في حكمها بإبعاده عن الدولة، أو الحكم بالإبعاد بدلاً من الحكم عليه بالعقوبة المقيدة للحرية"[122]، بيمنا كان النص القديم يقضي فقط بإبعاد الأجنبي الذي يُحْكَم عليه بالإدانة لارتكاب أي جريمة من الجرائم المنصوص عليها في هذا المرسوم بقانون، وذلك بعد تنفيذ العقوبة المحكوم بها.

ويرى الباحث أنه كان من الأفضل أن يظل الإبعاد مرتبطاً فقط بالعقوبة السالبة للحرية، أو على الأقل جعله جوازياً للقاضي، بحيث تكون له سلطة تقدير الحكم بالإبعاد أو الاكتفاء بالعقوبات الأصلية.

شروط تطبيق جزاء الإبعاد في قانون مكافحة جرائم تقنية المعلومات:

أوضح المشرع في نص المادة (20) من قانون مكافحة جرائم تقنية المعلومات شروط توقيع تدبير الإبعاد، وهي كالتالي:

---

(122) عُدل نص المادة (121) بموجب المادة (1) من القانون الاتحادي رقم 34 لسنة 2005، ثم أُستبدل بموجب المادة (1) من المرسوم بقانون اتحادي رقم 7 لسنة 2016، كما أُضيف نص فقرة ثالثة جديدة لنص المادة المذكورة بموجب المادة (2) من المرسوم بقانون اتحادي رقم 4 لسنة 2019، ثم أُستبدل نص المادة بالكامل بموجب المادة (1) من المرسوم بقانون اتحادي رقم 15 لسنة 2020.

1) صدور حكم من المحكمة المختصة.

2) أن يكون هذا الحكم صادراً بالإدانة، ويستوي أن تكون العقوبة سالبة للحرية أو الغرامة.

3) أن يكون الحكم صادراً بشأن ارتكاب جناية أو جنحة.

4) أن يكون المحكوم عليه من غير أبناء دولة الإمارات العربية المتحدة.

5) لا يتم تنفيذ الإبعاد إلا بعد انتهاء تنفيذ العقوبة أو انقضائها.

وبالنسبة لأسرة المبعد، فيتم ترحيلها عن الدولة إلا إذا كان أحد أفرادها من مواطني الدولة، فلا يجوز إبعاده، ومثال ذلك أن تكون زوجته تحمل جنسية الدولة.[123]

تطبيقات قضائية لمواجهة تدبير الإبعاد المشار إليه أعلاه:

في حكم محكمة النقض من الدائرة الجزائية، تتلخص وقائع الدعوى في أن النيابة العامة اتهمت المطعون ضده بأنه في يوم 12/ 2/ 2013 بدائرة أبوظبي دخل الى وسيلة تقنية المعلومات (جهاز حاسب آلي) والمملوك لشركة... بدون تصريح، وقام بنسخ البيانات المثبتة به، وإرسالها على بريده الإلكتروني على النحو المبين بالأوراق، وطلبت عقابه بالمواد (1، 2/ 2، 1، 3، 42) من المرسوم بقانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات. وقضت محكمة أبوظبي الابتدائية حضورياً بتاريخ 6/ 3/ 2013 بمعاقبته بالحبس لمدة شهرين والإبعاد، فاستأنف المتهم الحكم. وقضت محكمة استئناف أبوظبي حضورياً بتاريخ 17/ 4/ 2013 بإلغاء تدبير الإبعاد، وتأييد الحكم

(123) وفق التعديل الصادر بتاريخ 2019/8/14م للمرسوم بقانون اتحادي رقم (4) لسنة 2019 بتعديل بعض أحكام قانون العقوبات الصادر بالقانون الاتحادي رقم (3) لسنة 1987 في المادة (2)، والتي تنص "يُضاف إلى القانون الاتحادي رقم (3) لسنة 1987 بإصدار قانون العقوبات فقرة ثالثة للمادة (121)، ومادة برقم (359) مكرراً، وذلك على النحو الآتي: المادة (121) فقرة ثالثة: واستثناءً من نص الفقرتين السابقتين ومن أي نص ورد في أي قانون آخر، لا يجوز الحكم على الأجنبي بالإبعاد إذا كان زوجاً أو قريباً بالنسب من الدرجة الأولى لمواطن، وذلك ما لم يكن الحكم صادراً في جريمة من الجرائم الماسة بأمن الدولة".

المستأنف فيما عدا ذلك، ولما لم ترتضِ النيابة العامة هذا الحكم، فطعنت بطريق النقض بالطعن المطروح.

وقد بنت تعليلها في ذلك على: تنعي النيابة العامة على الحكم المطعون فيه أنه إذا أدان المطعون ضده بجريمة الدخول إلى وسيلة تقنية المعلومات المملوكة للغير بدون تصريح قد أخطأ في تطبيق القانون، ذلك أنه ألغى تدبير الإبعاد المقضي به من أول درجة رغم وجوبه بالنسبة للأجنبي عملاً بحكم المادة (42) من القانون رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات بما يعيبه ويستوجب نقضه.

ولما كانت المادة (42) من القانون رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات قد أوجبت على المحكمة أن تقضى بإبعاد الأجنبي الذي يُحَكَم عليه بالإدانة لارتكاب أي جريمة من الجرائم المنصوص عليها في هذا القانون بعد تنفيذ العقوبة المحكوم بها. ولما كان ذلك وكان الحكم المطعون فيه قد أدان المطعون ضده وهو أجنبي باكستاني الجنسية بالحبس لمدة شهرين، وأُلغى تدبير الإبعاد، فإنه يكون قد خالف القانون بما يوجب نقضه وتصحيحه بإضافة تدبير الإبعاد.[124]

[124] حكم المحكمة الاتحادية العليا، الطعن رقم 402 لسنة 2013 س 7 ق. أ، جلسة 22/ 5/ 2013، جزائي.

المطلب الرابع

الإشراف والمراقبة والحرمان من استخدام أي شبكة معلوماتية والإيداع في مأوى علاجي أو مركز تأهيل

نصت المادة (43) من المرسوم بقانون رقم 5 لينة 2012 بشأن مكافحة جرائم تقنية المعلومات على "مع عدم الإخلال بالعقوبات المنصوص عليها في هذا المرسوم بقانون يجوز للمحكمة أن تأمر بوضع المحكوم عليه تحت الإشراف أو المراقبة أو حرمانه من استخدام أي شبكة معلوماتية، أو نظام المعلومات الإلكتروني، أو أي وسيلة تقنية معلومات أخرى، أو وضعه في مأوى علاجي أو مركز تأهيل للمدة التي تراها المحكمة مناسبة".

وقد استحدثت هذه المادة مجموعة من التدابير للمحكمة أن تقضي بها بالإضافة للعقوبة الأصلية؛ فقد نصت على تدبير وضع المحكوم عليه تحت الإشراف أو المراقبة، وتدبير حرمانه من استخدام أي شبكة معلوماتية، أو نظام المعلومات الإلكتروني، أو أي وسيلة تقنية معلومات أخرى، وتدبير وضعه في مأوى علاجي أو مركز تأهيل للمدة التي تراها المحكمة مناسبة.

وللقاضي السلطة تقديرية بالنسبة للتدابير التي نصت عليها هذه المادة، وذلك من خلال القضاء بها من عدمه لأنها جوازية، والسلطة التقديرية للقاضي تكون من حيث الحكم بالتدبير، إضافة بأن توقيع التدابير للعقوبات المنصوص عليها في هذا المرسوم لا يمنع من تطبيق العقوبة الأصلية.[125]

ويرى الباحث أن مكافحة الإجرام وحماية المجتمع من الجريمة هي أهداف لا تتحقق بعقاب المجرم فقط، لأن العقوبة في بعض الأحيان لا تكفي وحدها للوفاء بهذه الأهداف في بعض الحالات، وهذا ما تم ملاحظته من خلال الازدياد المستمر في ظاهرة الإجرام، وارتفاع معدلات العودة للجريمة، وهو ما

(125) عبدالرزاق الموافي عبد اللطيف، شرح قانون مكافحة تقنية المعلومات، المرجع السابق، ص 152.

يدل على الاستهانة ببعض العقوبات في مواضع متعددة من أداء وظيفتها في حماية المجتمع من ظاهرة الإجرام، وقد كان هذا القصور دافعاً للتفكير في وسائل أخرى لمكافحة الإجرام لاستكمال مواطن النقص، وكانت هذه الوسيلة المكملة هي التدابير الاحترازية، فأصبحت العقوبة والتدابير الاحترازية وسيلتين متكاملتين لمكافحة الإجرام.

تطبيقات قضائية لمواجهة الجرائم المشار إليها في البحث ومنها:

<u>الواقعة الأولى:</u>

في حكم محكمة النقض – أبوظبي، الصادرة عند دائرة القضاء في إمارة أبوظبي، حيث تتلخص الوقائع في أن النيابة العامة أسندت إلى الطاعن... / أمريكي الجنسية أنه بتاريخ 10/ 4/ 2018م بدائرة أبوظبي، وبكونه من العاملين بمؤسسة... للطاقة النووية قد دخل إلى الموقع الإلكتروني الخاص بإحدى الجهات الحكومية، وذلك بقصد الحصول على بيانات حكومية ومعلومات سرية خاصة بالمؤسسة سالفة الذكر، وحصل على نسخة من هذه البيانات وأرسلها إلى البريد الإلكتروني الخاص به بدون الحصول على تصريح ممن يبيح له ذلك على النحو المبين بالتحقيقات، وطالبت النيابة العامة بمعاقبته بالمواد (1، 2/ 1 –2، 4، 41، 42) من المرسوم بقانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

وقضت محكمة أبوظبي الابتدائية بجلسة 2018/11/21م حضورياً بمعاقبة الطاعن بالسجن والغرامة والإبعاد، وبمصادرة الأجهزة وكافة الوسائل المستخدمة في ارتكاب الجريمة، وإغلاق البريد الإلكتروني الأربعة الخاصة به، ومحو كافة المعلومات والبيانات التي نسخها، وألزمته رسوم الدعوى الجزائية.

واستأنف المتهم على الحكم، وقضت محكمة الاستئناف بجلسة حضورياً بتاريخ 2018/12/21م بقبول الاستئناف شكلاً، وفي الموضوع بتعديل الحكم المستأنف إلى الاكتفاء بمعاقبة الطاعن بتخفيف

عقوبة السجن من سبع سنوات إلى أربع، وتأييده فيما عدا ذلك، وإلزامه بالرسوم القضائية، فطعن المتهم على الحكم، فقدمت النيابة العامة مذكرة بالرأي انتهت في ختامها أصلياً بنقض الحكم المطعون فيه، والقضاء مجدداً بعدم الاختصاص نوعياً، واحتياطياً برفض الطعن، ورأت المحكمة في غرفة المشورة أن الطعن جدير بالنظر، وحددت جلسة لنظره.

ودفع المتهم أمام محكمة الاستئناف بعدم اختصاصها الولائي بنظر الدعوى، وأن الاختصاص يعود إلى المحكمة الاتحادية العليا، غير أن المحكمة التفتت عن هذا الدفع، ولم ترد عليه رغم جوهريته، مما يعرض الحكم المطعون فيه للنقض، وبينت المحكمة أن التهمتان المنسوبتان للطاعن منصوص عليهما وعلى عقوبتهما في المادتين (2 و40) من المرسوم بقانون اتحادي رقم 5 لسنة 2012م في شأن مكافحة جرائم تقنية المعلومات.

وحيث إنه من المقرر أن الدفع بعدم الاختصاص يجوز إبداؤه في أي مرحلة تكون عليها الدعوى، وهو مسألة أولية يجب بحثها قبل الخوض في موضوع الدعوى، وأنه يتعين على محكمة الموضوع أن تجيب على كل دفاع يدلي به الخصوم، ويكون الفصل فيه مما قد يغير وجه الرأي في الدعوى.

ولما كان ذلك، وكان الثابت من الأوراق أن الطاعن دفع في صحيفة استئنافه بعدم اختصاص المحكمة ولائياً بنظر الدعوى على نحو ما أثاره بوجه النعي، ولم يعرض الحكم المطعون فيه لهذا الدفاع الجوهري الذي كان تحت يد وبصر المحكمة، وهو دفاع جوهري لو تحقق لتغير به وجه الرأي في الدعوى، فإنه يكون قد أخل بحق الدفاع بما يتعين نقضه.[126]

[126] محكمة النقض في دائرة القضاء، الطعن رقم 134 لسنة 2019 س 13 ق. أ، جلسة 2019/3/10، جزائي.

الواقعة الثانية:

في حكم المحكمة الاتحادية العليا، تتلخص الوقائع في أن النيابة العامة بتاريخ 2012/03/26 بدائرة أمن الدولة أسندت إلى المتهم... جريمة إنشاء موقع أو نشر معلومات على شبكة المعلومات أو إحدى وسائل تقنية المعلومات لترويج برامج وأفكار مخلة بالآداب العامة والنظام العام وإلقاء الرعب بين الناس مستوجباً الملاحقة القانونية عملاً بأحكام قانون مكافحة جرائم تقنية للمعلومات، وجريمة إثارة الأخبار أو البيانات أو الإشاعات الكاذبة أو المغرضة بالإذاعة بها، بقصد بث دعاية مثيرة من شأنها تكدير الأمن العام، وإلقاء الرعب بين الناس، أو إلحاق الضرر بالمصلحة العامة، وطالبت بمعاقبته بالمواد (1/82، 197، 198 مكرر فقرة 1) من قانون العقوبات الاتحادي المعدل بالقانون رقم 34 لسنة 2005 والمواد (20، 24، 26) من القانون رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات.

ورأت المحكمة أن ما قام به المتهم يوفر في حقه الأركان المادية والمعنوية لجريمتي الاتهام الواردتين بالمادة (20) من القانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات والمادة (198 مكرر فقرة 1) من قانون العقوبات الاتحادي، مما يتوجب معاقبته، وقضت بمصادرة الكمبيوتر (لاب توب) من نوع توشيبا والقرصين المدمجين المضبوطين.

ومن جهة أخرى ومراعاة لظروف المتهم الشخصية، فإن المحكمة تعامله بشيء من الرحمة، وتخفف عنه العقوبة إعمالا للمادة (98) من قانون العقوبات الاتحادي[127].

[127] المحكمة الاتحادية العليا، القضية رقم 2 لسنة 2012، جلسة بتاريخ 2012/03/26.

الواقعة الثالثة:

في حكم المحكمة الاتحادية العليا، تتلخص وقائع الدعوى في أن النيابة العامة بدائرة أبوظبي أسندت بتاريخ 2017/11/11م إلى المتهمين 1-... 2-... 3-... حال كون أحد المتهمين مكلفاً بخدمة عامة، والثالثة موظفاً عاماً، وبحكم مهنتهما كانا مستودعاً للسر أثناء وبمناسبة تأديتهم لوظيفتهم فأفشاه باستخدام وسيلة تقنية معلومات، وذلك على النحو المبين بالتحقيقات، واستخدما إحدى وسائق تقنية المعلومات (هاتفها المتحرك) في كشف معلومات سرية حصلتا عليها بمناسبة عملهما وبسببها، وطالبت النيابة معاقبتهم بالمواد (1، 20/ 1/ 22/ 41/ 46/ 1) من المرسوم رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، وقضت محكمة أبوظبي الابتدائية حضورياً بمعاقبتهم بالسجن والغرامة ومصادرة أدوات الجريمة، فاستأنفت المحكوم عليهم. وقضت محكمة استئناف أبوظبي حضورياً في 12/30/ 2018م بقبول الاستئنافات شكلاً، وتخفيف أحكام السجن عليهم جميعاً، فطعن وكيل المحكوم عليها/ الثالثة في 2019/1/17م، وطعن وكيل المحكوم عليه/ الأول في 2019/1/29م، كما طعن وكيل المحكوم عليها/ الثانية في 2019/1/29م.

أولاً: الطعن رقم 87/ 2019: جاء هذ الطعن مبنياً على أن المتهمة مريضة بمرض الذي يفقدها الشعور والإدراك، مما تنتفي معه مسؤوليتها الجنائية، وطلب الإحالة إلى لجنة طبية مختصة لبيان حالتها المرضية زمن الواقعة، إلا أن الحكم المطعون فيه أدانها، حيث تبين من الاطلاع على المفردات المضمونة أن المدافع عن الطاعنة تقدم بمذكرتي أمام درجتي التقاضي ضمنها عرضها على إحدى اللجان الطبية المختصة لبيان مدى سلامة قواها العقلية، وبفقدها الشعور والإدراك.

ولما كان ذلك، وكان من المقرر طبقاً لنص المادة (60) من قانون العقوبات الاتحادي التي تنص على "لا يسأل جنائياً من كان وقت ارتكاب الجريمة فاقداً الإدراك أو الإرادة لجنون أو عاهة في العقل أو غيبوبة ناشئة عن عقاقير أو مواد مخدرة أو مسكرة أياً كان نوعها أعطيت له قسراً عنه أو تناولها

بغير علم منه بها أو لأي سبب آخر يقرر العلم أنه يفقد الإدراك أو الإرادة، أما إذا لم يترتب على الجنون أو العاهة العقلية أو العقاقير أو المواد المخدرة أو المسكرة أو غيرها سوى نقص أو ضعف في الإدراك أو الإرادة وقت ارتكاب الجريمة، عُد ذلك عذراً مخففاً"، فإن هذا الدفاع من الطاعنة كان مطروحاً على المحكمة عند نظر موضوع الدعوى، وهو ما يُعد دفاعاً جوهرياً.

ولما كانت المحكمة لم تفعل ذلك، فإن حكمها يكون مشوباً بعيب القصور في التسبيب والإخلال بحق الدفاع، مما يبطله ويوجب نقضه للطاعنة وللطاعنين الآخرين لوحدة الواقعة، وحسن سير العدالة، دون حاجة لبحث باقي أوجه الطعن المقدمة من الطاعنة.

ثانياً: الطعنان رقما 128، 134/ 2019: لما كان الطعنان مرتبطين بالطعن رقم 2019/87، وكانت هذه المحكمة قد انتهت في هذا الطعن إلى نقض الحكم المطعون فيه، وتحديد جلسة لنظر الموضوع بالنسبة لجميع الطاعنين لوحدة الواقعة، وحسن سير العدالة، فلا حاجة إلى بحث أوجه تلك الطعون.[128]

(128) محكمة النقض، الطعون أرقام (87، 128، 132) لسنة 2018، س13 ق. أ، جلسة تاريخ 2019/02/20، هكذا ورد بالأصل سنة الطعون تارة بسنة 2018، وتارة أخرى بسنة 2019، ويرى الباحث صحتها 2019.

الخاتمة

تناول موضوع الدراسة تحليل الجرائم الماسة بأمن الدولة ومصالحها وفق قانون مكافحة جرائم تقنية المعلومات، لمواكبة الجرائم المستحدثة في الفضاء الإلكتروني، وللخطورة الكبيرة التي قد تنشأ عن هذه الجرائم، والتي من شأنها الإضرار بأمن الدولة داخلياً وخارجياً، وهو ما تمر به كثير من الدول في الفترة الحالية، والتطورات التي مرت وتمر بها منطقة الشرق الأوسط وشمال أفريقيا من تحول سياسي ومظاهرات ما هي إلا نتاج ممارسات غير مشروعة، كان يعتقد البعض بأنها حقوق وحريات، كما أنها عكست مدى التخلف والجهل والذي أدى في النهاية للانحياز إلى طوائف وتيارات خبيثة.

ولخطورة هذه الجرائم قام الباحث بالتركيز على الجرائم التي نص عليها القانون فيما يخص الجرائم الماسة بأمن الدولة ومصالحها ونصوص التشديد فيها، وقد تناولت الدراسة تعريف الجريمة الإلكترونية في المبحث التمهيدي، ثم تناولت في الفصل الأول المواجهة التشريعية للجرائم الإلكترونية الماسة بأمن الدولة، وبينت الفرق بين الجرائم الماسة بأمن الدولة الداخلي والخارجي حسب نص القانون في شأن مكافحة جرائم تقنية المعلومات بأركانها المادية والمعنوية، مع تناول أسباب تشديد العقوبة فيها.

ثم تناولت الدراسة في الفصل الثاني السياسة العقابية لمواجهة الجرائم الإلكترونية الماسة بأمن الدولة ومصالحها، مع بيان الاختصاص القضائي لهذه الجرائم، وكذلك والتدابير العقابية التي نص عليها القانون، وقد توصلت لعدد من النتائج والتوصيات، نستعرضها على النحو التالي:

أولاً: النتائج:

1) دوافع الجرائم الإلكترونية متعددة، وأهمها دوافع الانتقام والتحريض على الفوضى، وتحريك الشارع العام ضد سياسات الدولة بما يخدم المصالح الأجنبية المعادية.

2) كان إصدار قانون مكافحة جرائم تقنية المعلومات في عام 2006، والذي تم تعديله في العام 2012، وتعديل بعض نصوصه في العام 2018 نقلة استباقية للتطور الإلكتروني، وتطور الجريمة الإلكترونية.

3) في ظل تعدد مفهوم الجريمة الإلكترونية سيظل هناك إشكالية في وصف الجريمة، وذلك لتطورها عبر مرور الزمن.

4) إن تفعيل القضاء الإماراتي للمادة (2/16) من قانون العقوبات المتعلقة بالاختصاص يساعد على توسيع اختصاص المحاكم الإماراتية للنظر في هذا النوع من القضايا، وشمولها لأكبر عدد منها لمجرد حصول أي ضرر للمجني عليه أو نتيجة تمسه ضمن إقليم الدولة، مما يؤدي لزيادة الردع في هذه الجرائم، وعدم السماح لمرتكبيها بالإفلات من العقوبة لمجرد أن النشر تم خارج الدولة.

5) اتبع قانون دولة الإمارات العربية المتحدة بشأن مكافحة جرائم تقنية المعلومات أسلوب التشديد في الجرائم الإلكترونية بشكل عام، وخاصة في الجرائم الماسة بأمن الدولة، حيث اعتبر كافة هذه الجرائم جنايات.

6) حصر المشرع الإماراتي الجرائم الواردة في المواد التي تم ب في الدراسة، مع الإشارة إلى أن جميع المواد التي نص عليها القانون وارتكبت لصالح منظمة أجنبية أو دولة معادية تُعتبر من الجرائم الماسة بأمن الدولة.

7) جَرّم المشرع كافة صور النشر أو إعادة النشر بأي طريقة كانت عبر وسيلة تقنية المعلومات التي من شأنها التعرض لأمن الدولة.

8) الجرائم الماسة بأمن الدولة ومصالحها متشابهة في نتيجتها، ولكنها مختلفة بامتداد أضرارها.

9) اشترط المشرع الإعفاء من العقاب أو التخفيف بناءً على التبليغ عن جرائم أمن الدولة، مقترناً بطلب مُقَدَم من النائب العام.

ثانياً: التوصيات:

انتهي الباحث في هذه الدراسة إلى مجموعة من التوصيات كالتالي:

1) صياغة النصوص بعقوبات محددة، وعلى أن يتم أسلوب التشديد في حال نتج عن ذلك ضرر أو مساس بمصالح الدولة وكيانها، وذلك من منظور التوازن بين العقوبات التي فرضها المشرع.

2) إعادة النظر في المادتين (28 و29) من المرسوم بقانون رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، والمعدل بمرسوم بقانون اتحادي رقم 2 لسنة 2018، وذلك لتداخل مضمونها مع بعضها البعض.

3) تعديل قانون تقنية المعلومات، وتطبيق التدابير وفق القانون دون ترك بعض التدابير الاحترازية ليمكن تطبيقها على المتهمين الذين حصلوا على إعفاء من العقاب، وذلك مثل تطبيق مراقبة الشرطة وغيرها من التدابير، مثال ... (والمراقبة لمدة ... بعد تنفيذ العقوبة)

4) وضع إجراءات خاصة استثنائية في جميع الجرائم التي تمس أمن الدولة ومصالحها، تضمن عدم انقضاء الدعوى الجزائية وعدم سقوطها.

5) التوسع في فرض المزيد من القيود على مواقع التواصل الاجتماعي في الشق الخاص بأمن الدولة، سعياً للتضييق على الدول المعادية والمنظمات المشبوهة، ومواجهة مخاطر تزايد احتمالات ارتكاب الجرائم التي تمس بأمن الدولة ومصالحها، خاصة بعد الثورات التي شهدها الشرق الوسط وشمال أفريقيا، والتي لم تحصد منها الدول إلا انعدام الأمن، فضلاً عن بعض المشكلات التي لم تجد لها حلولاً.

6) توعية الأشخاص بأسباب حدوث الجرائم المعلوماتية وكيفية تنفيذها، ويكون للإعلام دور هام في توعية المواطنين عن مدى خطورة الجرائم الإلكترونية، كما يجب الإشارة أيضاً إلى كيفية التعامل معها والحماية منها.

7) محاربة الجريمة الإلكترونية تحتاج تكاتفاً من قِبل الدولة وأفراد مجتمعها حتى يمكن التصدي لها.

8) إنشاء منظمات لمكافحة الجريمة الإلكترونية.

قائمة المراجع

أولاً: المراجع العربية:

1) إبراهيم شاطر محمد الجبوري، جرائم الاعتداء على أمن الدولة من الداخل والخارج، المركز القومي للإصدارات القانونية، القاهرة، الطبعة الأولى، 2011.
2) أحمد غانم سيف السويدي، المواجهة الجنائية والأمنية للجرائم الماسة بأمن الدولة الداخلي، رسالة ماجستير، أكاديمية شرطة دبي، دبي، 2015.
3) أحمد فتحي سرور، الوسيط في قانون العقوبات، دار النهضة العربية، القاهرة، الطبعة السادسة، 2015.
4) أمير فرح يوسف، الجريمة الإلكترونية والمعلوماتية وجرائم الإنترنت، مكتبة الوفاء القانونية، الإسكندرية، الطبعة الأولى، 2011.
5) بدر الخبيزي، الجرائم الإلكترونية من وجهة نظر اجتماعية، دار دريم بوك، الكويت، الطبعة الثانية، 2017.
6) حسن محمد ربيع، شرح قانون العقوبات الاتحادي: القسم العام، الجزء الثاني، أكاديمية شرطة دبي، دبي 2005.
7) حسين بن سعيد الغافري، منظومة سلطنة عمان في التشريعات لمكافحة جرائم تقنية المعلومات، دار النهضة العربية، القاهرة، 2011.
8) حوراء موسى، الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، دار النهضة العربية، القاهرة، 2018.
9) خالد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت: دار الثقافة، عمّان، الطبعة الأولى، 2011.
10) راشد بشير إبراهيم، التحقيق الجنائي في جرائم تقنية المعلومات: دراسة تطبيقية على إمارة أبوظبي، مركز الإمارات والبحوث الاستراتيجية، أبوظبي، العدد 131، 2008.
11) رشدي محمد علي، الحماية الجنائية الموضوعية للمعلومات عبر شبكة الإنترنت، دار النهضة العربية، القاهرة، 2013.
12) رضا الغزاوي، عقوبة الإعدام في الوطن العربي، المنظمة المصرية للإصلاح الجنائي، القاهرة، 2007.
13) رمسيس بهنام، النظرية العامة للقانون الجنائي، منشاة المعارف، الإسكندرية، 1995.

14) سامي علي عياد حامد، الجريمة المعلوماتية وإجرام الإنترنيت، دار الفكر الجامعي، الاسكندرية، 2007.
15) سعد إبراهيم الأعظمي، موسوعة الجرائم الماسة بأمن الدولة الداخلي، دار الشؤون الثقافية العامة، بغداد، 2000.
16) سليمان عبد المنعم، مبادئ علم الجزاء الجنائي، دار الجامعة الجديدة، الإسكندرية، 2002.
17) سليمان محمد الطماوي، الوحدة الوطنية، الهيئة المصرية العامة للكتاب، القاهرة، 1979.
18) طارق أحمد فتحي سرور، الحماية الجنائية لأسرار الأفراد في مواجهة النشر، دار النهضة العربية، القاهرة، 2001.
19) طارق سرور، جرائم النشر والإعلام، دار النهضة العربية، القاهرة، الطبعة الأولى، 2004.
20) عبد الرزاق الموافي عبد اللطيف، شرح قانون مكافحة تقنية المعلومات، معهد دبي القضائي، دبي، 2014.
21) عبد العظيم مرسي وزير، شرح قانون العقوبات: القسم العام، الجزء الأول، دار النهضة العربية، القاهرة، الطبعة الرابعة، 2006.
22) علاء الدين منصور، الأوجه الحديثة للجرائم المعلوماتية، جامعة الحكمة، بيروت، 2000.
23) علي محمود علي حمودة، قانون العقوبات: النظرية العامة للجريمة، أكاديمية شرطة دبي، دبي، الطبعة الثانية، 2008.
24) عماد مجدي عبد الملك، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2011.
25) عمر حامد شكر، المجال الخامس: الفضاء الإلكتروني (دراسات استراتيجية)، المعهد المصري للدراسات، القاهرة، 2019.
26) غنام محمد غنام، فتيحة محمد قوراري، المبادئ العامة في قانون الإجراءات الجزائية لدولة الإمارات العربية المتحدة، دار الآفاق المشرقة، الشارقة، 2011.
27) فهد يوسف الكساسبة، وظيفة العقوبة ودورها في الإصلاح والتأهيل، دار وائل، عمّان، 2010.
28) لينا جمال محمد، الجرائم الإلكترونية، دار خالد الليحاني، عمّان، 2016.
29) مأمون سلامة، قانون العقوبات القسم العام، دار الفكر العربي، القاهرة، الطبعة الثالثة، 1990.
30) محمد أبو العلا عقيدة، أصول علم العقاب: دراسة تأصيلية للنظام العقابي الإسلامي والأنظمة العقابية المعاصرة مقارنة بالنظام العقابي في دولة الإمارات العربية المتحدة، جامعة الإمارات العربية المتحدة، العين، 1999.

31) محمد أحمد الحمادي، تشريعات مكافحة جرائم تقنية المعلومات في دولة الإمارات العربية وأحكام القضاء، بحوث ندوة شبكات الإنترنيت وتأثيراتها الاجتماعية والأمنية، القيادة العامة لشرطة أبوظبي، أبوظبي، 2006.
32) محمد الأمين البشري محجوب، إبراهيم حمد الهنائي، عادل عبدالله حميد، الجرائم الإلكترونية ودور أجهزة العدالة الجنائية من مواجهتها، وزارة الثقافة وتنمية المعرفة، أبوظبي، 2018.
33) محمد سالم الزعابي، الجرائم الواقعة على السمعة عبر تقنية المعلومات الإلكترونية، رسالة ماجستير، كلية الشرطة، أبوظبي، 2014.
34) محمد عبدالله العوا، الاحتيال عبر الإنترنت وجرائم بطاقات الائتمان، دار النهضة العربية، القاهرة، الطبعة الأولى، 2018.
35) محمود نجيب حسني، علم العقاب، دار النهضة العربية، القاهرة، الطبعة الثالثة، 1973.
36) مسعد علي الصباحي الكندي، القانون الواجب التطبيق على الجريمة الإلكترونية، أوراق للنشر والتوزيع، الشارقة، 2019.
37) ممدوح خليل عمر، حماية الحياة الخاصة والقانون الجنائي، دار النهضة العربية، القاهرة، 1983.
38) نواف كنعان، النظام الدستوري والسياسي لدولة الإمارات العربية المتحدة، مكتبة الجامعة، الشارقة، الطبعة الثانية، 2006.
39) وجيه الدسوقي المرسي، الأساليب الإلكترونية الحديثة التي تستخدمها التنظيمات الإرهابية في الجرائم الإرهابية، ندوة دور مؤسسات المجتمع المدني في التصدي للإرهاب، جامعة نايف العربية للعلوم الأمنية 2016/08/26.

ثانياً: المواقع الإلكترونية:

1) شبكة المحامين العرب.

https://www.mohamoon-ju.com/Default.aspx?action=QAAllJP&FIID=1453&Court=344

2) صفحة بن نخيره ومشاركوه، مقال د. عبد الوهاب عبدول، مختصر في جرائم أمن الدولة والمحكمة المختصة بنظرها.

https://www.lianapress.ae/releases/finance/d8-a7-d9-84-d9-85-d8-ae-d8-aa-d8-b5-d8-b1-d9-81-d9-8a-d8-ac-d8-b1-d8-a7-d8-a6-d9-85-d8-a7-d9-85-d9-86-d8-a7-d9-84-d8-af-d9-88-d9-84-d8-a9-d9-88-d8-a7-d9-84-d9-85-d8-ad-d9-83-d9-85-d8-a9-d8-a7-d9-84-d9-85-d8-ae-d8-aa-d8-b5-d8-a9-d8-a8-d9-86-d8-b8-d8-b1-d9-87-d8-a7.html

ثالثاً: القوانين والتشريعات:

1) المرسوم بقانون اتحادي رقم 15 لسنة 2020 بتعديل بعض أحكام قانون العقوبات الصادر بالقانون الاتحادي رقم 3 لسنة 1987.
2) المرسوم بقانون اتحادي رقم 4 لسنة 2019 بتعديل بعض أحكام قانون العقوبات الصادر بالقانون الاتحادي رقم 3 لسنة 1987.
3) المرسوم بقانون اتحادي رقم 2 لسنة 2018 بتعديل بعض أحكام المرسوم بقانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.
4) القانون الاتحادي رقم 2 لسنة 2018 في شأن قانون مكافحة جرائم تقية المعلومات.
5) المرسوم بقانون اتحادي 11 لسنة 2016 بشأن تعديل بعض أحكام القانون الاتحادي رقم 3 لسنة 1983 في شأن السلطة القضائية الاتحادية.
6) المرسوم بقانون اتحادي رقم 7 لسنة 2016م بتعديل بعض أحكام قانون العقوبات الصادر بالقانون الاتحادي رقم 3 لسنة 1987م.
7) القانون الاتحادي رقم 7 لسنة 2014 في شأن مكافحة الجرائم الإرهابية.
8) المرسوم بقانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.
9) القانون رقم 2 لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات.
10) القانون الاتحادي رقم 34 لسنة 2005 بتعديل بعض أحكام قانون العقوبات الصادر بالقانون الاتحادي رقم 3 لسنة 1987.
11) القانون الاتحادي رقم 35 لسنة 1992 بإصدار قانون الإجراءات الجزائية وتعديلاته.
12) قانون العقوبات الاتحادي رقم 3 لسنة 1987.
13) القانون الاتحادي رقم 3 لسنة 1983 بشأن السلطة القضائية الاتحادية.
14) المرسوم بقانون اتحادي رقم 3 لسنة 1983 بشأن السلطة القضائية الاتحادية.

رابعاً: القرارات الوزارية:

1) القرار الوزاري رقم (220) لسنة 2017 بإنشاء النيابة الاتحادية لجرائم تقنية المعلومات ومقرها في العاصمة أبوظبي.

خامساً: أحكام المحاكم:

1) حكم المحكمة الاتحادية العليا، الطعن رقم 402 لسنة 2013 س 7 ق. أ، جلسة 22/ 5/ 2013، جزائي.
2) حكم محكمة استئناف دبي رقم 2003/1248، جزائي.
3) الطعن 16 لسنة 2 ق، محكمة تمييز رأس الخيمة الدائرة الجزائية، جلسة 2007/10/21.
4) المحكمة الاتحادية العليا، طعن رقم 103 لسنة 31 قضائية.
5) المحكمة الاتحادية العليا، القضية رقم 2 لسنة 2012، جلسة بتاريخ 2012/03/26.
6) محكمة النقض في دائرة القضاء، الطعن رقم 134 لسنة 2019 س 13 ق. أ، جلسة 2019/3/10، جزائي.
7) محكمة النقض، الطعون أرقام (87، 128، 132) لسنة 2018، س13 ق. أ، جلسة تاريخ 2019/02/20، هكذا ورد بالأصل سنة الطعون تارة بسنة 2018، وتارة أخرى بسنة 2019، ويرى الباحث صحتها 2019.

سادساً: المراجع الأجنبية:

1) Cyberdiplomacy, shaun riordan, clays Ltd, London, 2019.

قائمة المحتويات

الموضوع	الصفحة
إقرار الباحث	أ
الإهداء	ج
الشكر والتقدير	د
الملخص باللغة العربية	هـ
الملخص باللغة الإنجليزية The Summary	ز
المقدمة	ح
المبحث التمهيدي: مفهوم الجرائم الإلكترونية الماسة بأمن الدولة	1
المطلب الأول: ماهية الجرائم الإلكترونية	3
المطلب الثاني: أركان الجرائم الإلكترونية الماسة بأمن الدولة	10
الفرع الأول: الركن المادي في الجرائم الإلكترونية	13
الفرع الثاني: الركن المعنوي في الجرائم الإلكترونية	15
الفصل الأول: المواجهة التشريعية للجرائم الإلكترونية الماسة بأمن الدولة	18
المبحث الأول: الجرائم الإلكترونية الماسة بالأمن الداخلي	20
المطلب الأول: نطاق جرائم أمن الدولة الداخلي	21
المطلب الثاني: أنواع الجرائم الإلكترونية الماسة بأمن الدولة الداخلي	28
الفرع الأول: جرائم الدخول بدون تصريح بقصد الحصول على بيانات حكومية	29
الفرع الثاني: جرائم إثارة الفتنة أو الكراهية أو العنصرية أو الإضرار بالوحدة الوطنية أو السلم الاجتماعي	33
الفرع الثالث: الجرائم المتعلقة بتعريض أمن الدولة ومصالحها للخطر والمساس بالنظام العام	37

الفرع الرابع: الجرائم المتعلقة بالسخرية أو الإضرار بسمعة وهيبة ومكانة الدولة أو أي من مؤسساتها أو رئيسها أو حكامها أو أولياء عهودها أو علمها أو سلامها الوطني أو رموزها	41
الفرع الخامس: الجرائم المتعلقة بقلب نظام الحكم في الدولة أو الاستيلاء عليه أو تعطيل أحكام الدستور أو القوانين السارية في البلاد	43
المبحث الثاني: الجرائم الإلكترونية الماسة بالأمن الخارجي	46
المطلب الأول: نطاق جرائم أمن الدولة الخارجي	47
المطلب الثاني: أنواع الجرائم الإلكترونية الماسة بأمن الدولة الخارجي	54
الفرع الأول: الجرائم المتعلقة بالجماعات الإرهابية أو الهيئات غير المشروعة	55
الفرع الثاني: الجرائم المتعلقة بتقديم معلومات عير صحيحة أو غير دقيقة من شأنها الإضرار بمصالح الدولة	60
الفصل الثاني: السياسة العقابية لمواجهة الجرائم الإلكترونية الماسة بأمن الدولة ومصالحها	64
المبحث الأول: نطاق الاختصاص القضائي بنظر الجرائم الإلكترونية الماسة بأمن الدولة	65
المبحث الثاني: العقوبات والتدابير الاحترازية لمواجهه الجرائم الماسة بأمن الدولة ومصالحها	73
المطلب الأول: المصادرة	78
المطلب الثاني: إغلاق المحل أو الموقع الذي ارتكبت فيه الجريمة	80
المطلب الثالث: إبعاد الأجنبي	82
المطلب الرابع: الإشراف والمراقبة والحرمان من استخدام أي شبكة معلوماتية والإيداع في مأوى علاجي أو مركز تأهيل	86
الخاتمة	92
النتائج	91
التوصيات	92
قائمة المراجع	96
قائمة المحتويات	101