البنيان القانوني لجريمة اختراق المواقع الحكومية على ضوء أحكام المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١

دراسة تحليلية مقارنة

The legal structure of the crime of hacking government websites in light of the provisions of Federal Decree-Law No. (34) of 2021 - a comparative analytical study

فاطمة سالم عبدالله محمد – طالبة ماجستير في القانون العام – جامعة الشارقة

د. حليمة خالد المدفع – استاذ مساعد في القانون الجنائي – جامعة الشارقة

د. وليد النيباري– رئيس النيابة العامة – دبي

الملخص

تناولت الدراسة موضع البنيان القانوني لجريمة اختراق المواقع الحكومية، وذلك نظراً لخطورة هذه الجريمة على الأنظمة المعلوماتية الحكومية، حيث تناولت الدراسة بالتحليل ماهية الاختراق، وأنواعه، وبينت أركان جريمة الاختراق، والعقوبات الأصلية والتكميلية التي نص عليها المشرع الإماراتي في المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن الشائعات والجرائم الإلكترونية.

حيث أن هناك مشكلة تتمثل في التداخل بين الأفعال المكونة للاختراق والتي تكون السلوك الإجرامي في الركن المادي للجريمة وبين بعض الأفعال الأخرى القريبة من الاختراق مثل التعطيل والاعتراض.

تتمثل أهمية الدراسة في أنها تسلط الضوء على ماهية المواقع الإلكترونية الحكومية وتمييزها عن غيرها من المواقع الأخرى مع البحث في أركان الجريمة وعقوبتها على ضوء أحكام المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن الشائعات والجرائم الإلكترونية، والمقارنة مع موقف المشرع المصري في القانون رقم (١٧٥) لسنة ٢٠١٨ بشأن جرائم تقنية المعلومات، كما أن الدراسة تبين الإطار النظري للجريمة من حيث التجريم والعقاب. كما أنها تبين الإطار العلمي للجريمة من حيث خصوصية أركانها وخصوصية العقوبات التي أفردها المشرع لها، كما تعتبر الدراسة من أوائل الدراسات التي تختص بنوع واحد من الجرائم الواقعة على المواقع الإلكترونية الحكومية على ضوء المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ حيث انها سوف تقدم العديد من التوصيات التي تسهم في سد الثغرات القانونية في القانون إن وجدت

وتوصلت الدراسة لنتيجة مفادها: المشرع الإماراتي أخذ بمبدأ تشديد العقوبة على جريمة اختراق الأنظمة المعلوماتية للمؤسسات الحكومية في حال نتج عنها أي من النتائج السابقة، وهنا يمكن القول بأن الأحكام الخاصة بجريمة اختراق الأنظمة المعلوماتية للمؤسسات الحكومية تميل إلى التشديد وفق النتيجة الإجرامية التي تنتج عن فعل الاختراق ذاته.

ومن توصيات الدراسة: على المشرع الإماراتي أن يضع جريمة الاختراق المعلوماتي وحدها كجريمة مستقلة عن باقي الجرائم، كون ما ورد في القانون يخلط بين الاختراق والبقاء غير المشروع، كما تقترح الباحثة نصاً لهذه المادة على النحو الآتي:" الاختراق هو الهجوم الذي يتم خلاله الدخول للمنظومة المعلوماتية ويتسبب بالنتائج التالية: "الإتلاف" و"التدمير" و"التخريب" و "محو البرامج والبيانات" و"التشويه" و"مسح البرامج والبيانات" و"إيقاف" أو "حذف" أو أي سلوك آخر يجعل البيانات أو المعلومات أو البرامج والمحررات المعلوماتية غير صالحة للاستعمال كلياً أو جزئياً. "

الكلمات الدالة: النظام المعلوماتي- المؤسسات الحكومية- الاختراق- العقوبة- ظروف التشديد والتخفيف.

Abstract

The study dealt with the position of the legal structure of the crime of hacking government websites, due to the seriousness of this crime on government information systems, where the study analyzed the nature of penetration, its types, and showed the elements of the crime of hacking, and the original and complementary penalties stipulated by the UAE legislator in Federal Decree-Law No. (34) of 2021 regarding rumors and cybercrime. As there is a problem of overlap between the acts that make up the penetration, which constitute the criminal behavior in the material element of the crime, and some other acts close to penetration, such as disruption and interception.

The importance of the study is that it sheds light on the nature of government websites and distinguishes them from other sites with research into the elements and punishment of crime in light of the provisions of Federal Decree-Law No. (34) of 2021 regarding rumors and cybercrime, and a comparison with the position of the Egyptian legislator in Law No. (175) of 2018 on information technology crimes, and the study shows the theoretical framework of the crime in terms of criminalization and punishment. It also shows the scientific framework of the crime in terms of the privacy of its pillars and the privacy of the penalties allocated by the legislator to it, and the study is considered one of the first studies that specialize in one type of crime on government websites in light of Federal Decree-Law No. (34) of 2021, as it will provide many recommendations that contribute to filling the legal gaps in the law, if any. The study reached a conclusion that: the UAE legislator adopted the principle of tightening the penalty for the crime of penetrating the information systems of government institutions in the event that it resulted in any of the previous results, and here it can be said that the provisions for the crime of penetrating the information systems of government institutions tend to be tightened according to the criminal result that results from the act of penetration itself. Among the recommendations of the study: The UAE legislator should put the crime of information hacking alone as a crime independent of the rest of the crimes, because what is stated in the law confuses penetration and illegal survival, and the researcher also proposes a text for this article as follows: "Penetration is the attack during which access to the information system is carried out and causes the following results: "destruction", "destruction", "sabotage", "erasure of programs and data", "distortion", "erasure of programs and data", "stop", "deletion" or any other behavior that makes data or Information or software and information documents are not usable in whole or in part".

Keywords: information system - government institutions - penetration - punishment - aggravating and mitigating conditions.

مقدمة:

في ظل ثورة المعلومات والاتصالات أصبحت الحكومات أكثر اعتمادا على شبكة الإنترنت في إنجاز المعاملات الحكومية وتقديم الخدمات للمواطنين وتعتمد الحكومات بشكل عام على تقنيات تكنولوجيا المعلومات عبر شبكة من المواقع الإلكترونية الحكومية التي تتيح ميزة تقديم الطلبات الإلكترونية ومعالجتها وتقديم الخدمات ومتابعة المعاملات، وعلى الرغم من ذلك فأن وسائل تقنية المعلومات من الممكن أن تتعرض للاختراق عبر استخدام التقنيات الحديثة بشكل عام حيث يلجأ مرتكب جريمة اختراق المواقع الإلكترونية الحكومية إلى اتباع العديد من الطرق والوسائل لذلك، ولا سيما اعتراض المراسلات الحكومية أو تهكير المواقع الحكومية بهدف إعاقتها عن العمل أو التأثير عليها، وبما أن دولة الإمارات العربية المتحدة في مقدمة دول المنطقة والتي تعتمد كليا على شبكة المعلومات الحكومية في تقديم خدماتها في شتى المجالات ولا سيما عبر المواقع الحكومية على شبكة الإنترنت أو عبر التطبيقات الذكية فأن مسألة حماية المواقع الحكومية الإلكترونية من الجرائم أصبح الشغل الشاغل لدى الجميع

وعليه أصدر المشرع الإماراتي المرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١ بشأن الشائعات والجرائم الإلكترونية وفق المنظومة القانونية المتقدمة في دولة الإمارات العربية المتحدة، حيث يحتوي القانون على العديد من المواد التي تحتوي على. قواعد التجريم والعقاب على جريمة اختراق المواقع الحكومية وجاءت فكرة الدراسة من ضرورة توفير الحماية الجنائية للمواقع الحكومية في دولة الإمارات العربية المتحدة من الاختراق حيث أن هذه الجريمة تنطوي على خطورة كبيرة وقد تؤدي إلى تعطيل المواقع الحكومية وإيقاف العمل بها ، لذلك نجد أن المشرع الإماراتي أكثر حرصا على حماية هذه المواقع كما أن العقوبات الواردة في المرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١ تحقق الردع العام والردع الخاص لهذا النوع من الجرائم وعليه يمكن القول بأن جريمة الاختراق للمواقع الحكومية من الجرائم المستحدثة التي استحدث لها المشرع الإماراتي العديد من العقوبات الأصلية والتكميلية والفرعية

مشكلة الدراسة:

إن جريمة اختراق المواقع الإلكترونية الحكومية هي من الجرائم التي تنضوي على خطر كبير، لإمكانية الحصول على المعلومات والبيانات تتسم بالخصوصية أو السرية والتي قد يتم استغلالها في أغراض غير قانونية قد تؤثر سلبا على أداء الجهات الحكومية لأعمالها عبر المواقع الالكترونية، وعليه لابد أن تكون المواجهة الجنائية لهذا النوع من الجرائم أن تكون ذو فعالية للحد من هذه الجرائم كما أشرنا لخطورتها، وأيضا هناك مشكلة أخرى تتمثل في التداخل بين الأفعال المكونة للاختراق والتي تكون السلوك الإجرامي في الركن المادي للجريمة وبين بعض الأفعال الأخرى القريبة من الاختراق مثل التعطيل والاعتراض، عليه يمكن بلورة مشكلة الدراسة في التساؤل التالي: ما مدى فعالية قواعد التجريم والعقاب التي جاء بها المشرع الإماراتي في المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ في مواجهة خطر جريمة الاختراق الالكتروني؟

تساؤلات الدراسة:

١) ماهي المواقع الإلكترونية الحكومية، وما يميزها عن غيرها؟
٢) ماهي جريمة اختراق المواقع الإلكترونية الحكومية؟
٣) ماهي أركان جريمة اختراق المواقع الإلكترونية الحكومية؟
٤) ماهي العقوبات التي فرضها المشرع الإماراتي على مرتكبي جريمة الاختراق للمواقع الحكومية وما مدى فعاليتها في الحد من الجريمة؟

أهمية الدراسة:

تتمثل أهمية الدراسة في أنها تسلط الضوء على ماهية المواقع الإلكترونية الحكومية وتمييزها عن غيرها من المواقع الأخرى مع البحث في أركان الجريمة وعقوبتها على ضوء أحكام المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن الشائعات والجرائم الإلكترونية، والمقارنة مع موقف المشرع المصري في القانون رقم (١٧٥) لسنة ٢٠١٨ بشأن جرائم تقنية المعلومات، كما أن الدراسة تبين الإطار النظري للجريمة من حيث التجريم والعقاب. كما أنها تبين الإطار العلمي للجريمة من حيث خصوصية أركانها وخصوصية العقوبات التي أفردها المشرع لها، كما تعتبر الدراسة من أوائل الدراسات التي تختص بنوع واحد من الجرائم الواقعة على المواقع الإلكترونية الحكومية على ضوء المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ حيث انها سوف تقدم العديد من التوصيات التي تسهم في سد الثغرات القانونية في القانون إن وجدت.

أهداف البحث:

تسعى الباحثة من خلال الدراسة إلى تحقيق الأهداف التالية:

١) بيان ماهية المواقع الإلكترونية الحكومية وتمييزها عن غيرها من المفاهيم المشابهة.
٢) بيان أركان جريمة اختراق المواقع الإلكترونية الحكومية.
٣) تحديد أنواع العقوبات التي جاء بها المشرع الإماراتي بخصوص جريمة اختراق المواقع الإلكترونية الحكومية

منهجية البحث:

يعتمد البحث على المنهج الوصفي التحليلي، وذلك من خلال وصف موضوع البحث من الناحية النظرية من حيث المفاهيم والخصائص، ويسهم الوصف في بيان أدبيات موضوع البحث ورسم الخطوات التي يتم اتباعها في البحث، والمنهج التحليلي من خلال تحليل ما جاءت به مواد المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ من حيث التجريم والعقاب على جريمة اختراق المواقع الإلكترونية الحكومية، والمنهج المقارن من خلال المقارنة بين موقف المشرع الإماراتي والمشرع المصري في القانون رقم (١٧٥) لسنة ٢٠١٨ بشأن جرائم تقنية المعلومات.

سابعاً: تقسيم البحث

المبحث التمهيدي: الأحكام العامة لماهية جريمة الاختراق للمواقع الحكومية

- المطلب الأول: تعريف جريمة اختراق المواقع الإلكترونية الحكومية
- المطلب الثاني: خصوصية جريمة اختراق المواقع الإلكترونية الحكومية

المبحث الاول: أركان جريمة اختراق المواقع الالكترونية الحكومية

- المطلب الأول: الركن المادي لجريمة اختراق المواقع الإلكترونية الحكومية
- المطلب الثاني: الركن المعنوي لجريمة اختراق المواقع الإلكترونية الحكومية

المبحث الثاني: العقوبات والتدابير المقررة لجريمة الاختراق الالكترونية

- المطلب الأول: العقوبات الأصلية لجريمة اختراق المواقع الإلكترونية الحكومية
- المطلب الثاني: العقوبات التبعية والتكميلية لجريمة اختراق المواقع الإلكترونية الحكومية
- المطلب الثالث: ظروف التشديد والتخفيف والإعفاء من العقوبة لجريمة اختراق المواقع الإلكترونية الحكومية

المبحث الأول

الأحكام العامة لماهية جريمة اختراق المواقع الإلكترونية الحكومية

تمهيد وتقسيم:

نتناول في هذا المبحث البنيان القانوني لجريمة اختراق المواقع الإلكترونية من خلال المطالب التالية:

- **المطلب الأول: ماهية جريمة اختراق المواقع الإلكترونية الحكومية**
- **المطلب الثاني: خصوصية جريمة اختراق المواقع الإلكترونية الحكومية**

المطلب الأول

تعريف جريمة اختراق المواقع الإلكترونية الحكومية

عرف المشرع الإماراتي الاختراق في نص المادة الأولى من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن إصدار قانون مكافحة الشائعات والجرائم الإلكترونية بأنه:" الاختراق: الدخول غير المرخص به أو المخالف لأحكام الترخيص أو الدخول بطريقة غير مشروعة أو البقاء بصورة غير مشروعة في نظام معلوماتي أو حاسب آلي أو نظام تشغيل جهاز أو آلة أو مركبة أو شبكة معلوماتية وما في حكمها[٤]."

ومن هذا النص ترى الباحثة: أن المشرع الإماراتي قد بين ماهية الاختراق بأنه فقعل الدخول غير المشروع بشكل غير مرخص أو الدخول بترخيص لكن بشكل مخالف لأحكام الترخيص على أن يكون هذا الدخول للمواقع الإلكترونية الحكومية يتصف بعدم المشروعية، وحدد المشرع الإماراتي خلال التعريف محل الدخول غير المشروع بأن يكون إلى نظام الحاسب الآلي أو نظام التشغيل للآلات والأجهزة أو شبكة المعلومات أو أية شيء يكون بحكمها، وهنا يمكن القول بأن المشرع الإماراتي يعتبر الاختراق هو الفعل المجرم وأن الدخول غير المشروع إلى الأنظمة المعلوماتية هو الغاية أو الوسيلة لارتكاب جريمة الاختراق، وقد أحسن المشرع الإماراتي في تعريفه للاختراق على هذا النحو.

ويعرف المشرع المصري الاختراق في المادة الأولى من القانون رقم (١٧٥) لسنة ٢٠١٨ بشأن جرائم تقنية المعلومات بأنه: الاختراق: الدخول غير المرخص به أو المخالف لأحكام الترخيص، أو الدخول بأي طريقة غير مشروعة إلى نظام معلوماتي أو حاسب آلي أو شبكة معلوماتية وما في حكمها."

ومنه يتضح ان هناك توافق بين المشرع الإماراتي والمشرع المصري باعتبار الاختراق دخول غير مصرح به لنظام معلوماتي.

كما يعرف الاختراق بأنه:" هو الدخول بصورة غير مشروعة وغير قانونية إلى أجهزة الكمبيوتر وشركات الحاسبات والتي تتم من خلال توفر شبكة الإنترنت وبرامجها المتعددة.[٥]"

وهنا توصي الباحثة بأن يقوم المشرع الإماراتي بالفصل بين الاختراق والدخول غير المشروع لأن كل منهما يختلف عن الآخر، حيث إن الاختراق هو فعل سابق للبقاء غير المشروع.

ومنه ترى الباحثة أن جريمة الاختراق الإلكتروني هي مقدمة لجرائم أخرى، حيث أنه من غير المتصور أن ترتكب جريمة الاختراق دون أن يكون الهدف منها هو اتجاه إرادة مرتكب الجريمة إلى تحقيق نتيجة معينة من جراء الاختراق.

---

[٤] دولة الإمارات العربية المتحدة - مرسوم بقانون اتحادي - رقم ٣٤ لسنة ٢٠٢١ الصادر بتاريخ ٢٠٢١-٠٩-٢٠ نشر بتاريخ ٢٠٢١-٠٩-٢٦ يعمل به إعتبارا من ٢٠٢٢-٠١-٠٢ بشأن مكافحة الشائعات والجرائم الإلكترونية. الجريدة الرسمية ٧١٢ ملحق - السنة الواحد والخمسون

[٥] عبير شفيق الرحباني: الجرائم الإلكترونية ومخاطرها، دار الثقافة للنشر والتوزيع، عمان، ط١، ٢٠٢٠م، ص٢٠

ومن خلال ما ورد في المطلب الأول ترى الباحثة أن هناك تباين واختلاف في تعريف الاختراق ولا سيما أن جريمة الاختراق الإلكتروني تتم عبر تقنيات يعتمد عليها مرتكب الجريمة أكثر ما يقال عنها أنها برامج خبيثة، كما تلاحظ الباحثة أن هناك خلط بين عدة أفعال مثل الدخول غير المصرح به والولوج إلى البرامج المعلوماتية عن طريق الهاكرز وهنا توصي الباحثة بأن يقوم المشرع الإماراتي بإفراد مادة خاصة بتعريف الاختراق وبيان الأسباب المؤدية له ووسائله بمعزل عن بقية الأفعال الأخرى.

المطلب الثاني

خصوصية جريمة اختراق المواقع الإلكترونية الحكومية

تعرضت كثير من أنظمة الحاسبات الآلية، وبصفة خاصة تلك التي تعمل من خلال شبكات المعلومات إلى الاختراق بواسطة أشخاص غير مصرح لهم بالدخول إليها، وفي الولايات المتحدة الأمريكية، حيث كان الظهور الأول لهذه الظاهرة أطلق على هؤلاء الذين يدخلون إلى أنظمة الحاسبات الآلية بدون تصريح القراصنة قياساً على الأشخاص الذين كانوا يقومون في الماضي باعتراض البرامج الإذاعية[٦].

وتختلف الوسائل التي يمكن اللجوء إليها للدخول غير المصرح به إلى نظام الحاسب الآلي، وتفترض جميعها قدراً من المعرفة بتكنولوجيا الحاسبات الآلية[١]، وإن كانت تتراوح في مداها. ففي بعض الأحيان لا يتطلب الدخول أكثر من تشغيل الحاسب الآلي أو فتح البرنامج الذي يقوم بتشغيله[٧].

والحقيقة إن هناك تنوعاً للجريمة عبر الإنترنت إلا إنها جميعها تتحد في طبيعتها، بحيث يمكن القول إنه حتى التقليدي منها يتميز بخصوصية الانتماء إلى الإنترنت، هذا الانتماء هو سمة التطوير الذي لحق التجريم التقليدي عبر الإنترنت[٨]، والذي أشار إليه الفقه يكون الجريمة التقليدية إما أن ترتكب "بواسطة الإنترنت " وإما أن ترتكب على "الإنترنت "[٩].

ولهذا الرأي الوجيه أساس متقدم في الفقه المقارن حيث يذهب اتجاه في الفقه الإنجليزي إلى أن الجريمة المرتبطة قد تكون غير ذات علاقة بالإنترنت وإنما استخدمت الإنترنت لكي يتم ارتكابها بحيث تمثل الهدف الخفي للاختراق عبر الإنترنت ويأخذ القانون الإنجليزي ١٩٩٠م بهذا الاتجاه، فالقسم الثاني من القانون المذكور ينص على أنه "يعد الشخص مذنباً بجريمة في إطار هذا القسم إذا ارتكب جريمة في إطار القسم الأول أعلاه (جريمة الدخول غير المصرح به) بقصد:

أ- ارتكاب احدى الجرائم التي ينص عليها القسم المذكور، أو:

---

[٦] عبير شفيق الرحباني : الجرائم الإلكترونية ومخاطرها ، دار الثقافة للنشر والتوزيع، ط١، ٢٠٢٠م ، ص ٣٦

[١] Buffelan - Lanore: La Procédure Apllicable Aux Infraction Commises Par Les Personnes Morales Rev, Sociétés 1993. P. 315 ets.

[٧] راشد محمد المري : الجرائم الإلكترونية، دار النهضة العلمية ودار النهضة العربية ، مصر والإمارات ، ط١ ، ٢٠١٨م ، ص ٧٧

[٨] PETER SWIFT: HACK MAN MENACE OF THE KEYBOARD CRIMINAL BRITICH TELECOM WORLD MAG, HALF OF SEPT 1989 P 13-14.

[٩] جميل الصغير : جرائم الإنترنت، دار النهضة العربية، القاهرة، ٢٠١٤، ص ٢١٨

ب- لتسهيل ارتكاب مثل هذه الجرائم (سواءً بنفسه أو بواسطة شخص آخر): والجريمة التي يقصد ارتكابها أو تسهيل ارتكابها المشار إليها في عجز القسم المذكور يطلق عليها "الجريمة الغرضية ". والتي تشير إلى أن ارتكاب الجريمة عبر الإنترنت والحاسوب له هدف إجرائي آخر (تعدد الجرائم).

إن الهدف الرئيسي والأول لأمن المعلومات هو الحفاظ على استمرارية تدفق هذه المعلومات على المتلقي أو المستفيد، أما الهدف الثاني فهو حماية المعلومات الحساسة للمؤسسة الأمنية سواءً كانت تملكها أو تحت سيطرتها. والتخفي بانتحال صلاحيات شخص مفوض Masquerading بالدخول إلى النظام عبر استخدام وسائل التعريف العائدة لمستخدم مخول بهذا الاستخدام، كاستغلال كلمة سر[١١]، أحد المستخدمين، واسم هذا المستخدم، أو عبر استغلال نطاق صلاحيات المستخدم الشرعي يعد اختراقاً للمعلومات[١٢]

ومع أن هذا النمط من الاختراقات هو الشائع سواءً في البيئة الداخلية للمنشأة أو الخارجية، إلا أن وضعه ضمن طائفة الاختراقات المتصلة بالموظفين ومستخدمي النظام من الداخل يكون مصدر حصوله الغالب في هذه البيئة بسبب أخطاء تشارك الموظفين كلمات السر ووسائل التعريف، وبسبب الحصول عليها عن طريق استراق النظر أو نحو ذلك من الأساليب التي تتواجد في بيئة العمل الداخلي، وتتيح الحصول على كلمات المرور أو وسائل التعريف[١٣]
من أشهر القضايا في هذا المجال تلك الواقعة المشهورة وهي حادثة المواقع الاستراتيجية في فبراير ١٩٩٩م إدانة الأمريكي إيرك بورنس، من قبل محكمة فرجينيا الغربية بالحبس لمدة ١٥ شهراً، مع وضعه تحت مراقبة الشرطة لمدة ٣ سنوات، بعد اعترافه بالجرم الذي ارتكبه، إذ عمداً باختراق أجهزة الحاسب الآلي المحمية وألحق بها أضرار بالغة في الولايات المتحدة بولايتي فرجينيا وواشنطن بالإضافة إلى لندن ببريطانيا.[١٤]

وتعد مسئولية أمن المعلومات والتخطيط الوقائي موضوع مهم إلى حد كبير، والسبب في ذلك

ومن وقائع إحدى القضايا في دولة الإمارات العربية المتحدة:" تتحصل في أن النيابة العامة أحالت المطعون ضدهما للمحاكمة الجنائية بوصف أنهما بتاريخ سابق على ٢٠١١/٢/١٥ بدائرة خورفكان : استغلا خدمة من خدمات مؤسسة الاتصالات بأن قاما متعمدين بالدخول غير المشروع بشبكة الاتصالات وإجراء المكالمات الدولية على النحو الذي يخالف أحكام القانون . وطلبت معاقبتهما طبقاً للمواد ١ , ٧ , ٢/٤٢ , ٧٢ مكرراً , ٧٦ من القانون الاتحادي رقم ٣ لسنة ٢٠٠٣ والمعدل بالقانون الاتحادي رقم لسنة ٢٠٠٨ في شأن تنظيم قطاع الاتصالات[١٥]".

---

(١١) Guillaume Champy, La fraude informatique, tome 1, () Presses Universitaires d Aix-Marseille, 51992, p. 88.

(١٢) شمسان ناجي صالح الخيلي : الجرائم المستخدمة بطرق غير مشروعة لشبكة الإنترنت ـــ دار النهضة العربية – القاهرة – مصر – ٢٠١٩ – ص٣٤

(١٣) محمد الجندين مقال "خصائص البيانات الضخمة"، مجلة لغة العصر، جريدة الأهرام، العدد ٢٣٩، القاهرة، أكتوبر ٢٠١٦م.ص٣٤

(١٤) الدكتور محمود رجب فتح الله: الوسيط في الجرائم المعلوماتية دار الجامعة الجديدة الطبعة الأولى، سنة ٢٠١٨، ص ١ وما بعدها.

(١٥) المحكمة الإتحادية العليا - الأحكام الجزائية - الطعن رقم ١٨٥ لسنة ٢٠١١ قضائية بتاريخ ٢٠١١-٠٦-٢١ [رفض]

وتنفرد جريمة الدخول غير المشروع ببقاء بنيانها على أساس ثنائي على الرغم من أن الشارع المقارن اعتبرها في أغلب الأحيان جريمة شكلية؛ فالشارع يعاقب على مجرد الاختراق، ثم إنه في ذات الوقت يجعل من هذه الجريمة ثنائية الموضوع بشكل حتمي. وبيان ذلك أن الاختراق كجريمة شكلية يتطلب النفاذ إلى نظام حاسوب عبر الإنترنت، أي يقوم المخترق بنشاط الدخول دون أن يكون له صلاحية أو مشروعية في الدخول إليه. وتتحقق صورة عدم المشروعية في عدم صلاحية الدخول إلى نظام الحاسوب، وبصورة يبرز فيها المخترق كما لو كان ممن لا تتحقق فيهم شروط إلى نظام حاسوبي. فالأصل في الاختراق ليس كونه جريمة شكلية وإنما يعد جريمة ثنائية الطابع؛ إذ يوجد الاختراق، ثم بعد ذلك جريمة أو سلسلة الجرائم الأخرى التي يتم ارتكابها على إثر الاختراق، بمعنى أنه لا يمكن أن ينشأ عن الاختراق أي ارتباط بحسن النية ولو كان المخترق من دعاة السلام" هاكر"[١٦].

ومن الأحكام القضائية الواردة من محكمة التمييز في دولة الكويت:" ..دانها بجرائم استعمال الشبكة المعلوماتية في تهديد المجني عليه والدخول غير المشروع إلى موقع إلكتروني ترتب عليه حذف بيانات به ونشر ما من شأنه المساس بكرامة المجني عليه وإساءة استعمال وسيلة من وسائل الاتصالات الهاتفية قد شابه القصور في التسبيب والإخلال بحق الدفاع ، ذلك بأن المحكمة دانتها رغم خلو الأوراق من دليل يقيني في حقها ".[١٧]

ومن هذا الحكم يتضح أن جريمة الاختراق في هذه القضية تمت بهدف الدخول غير المشروع إلى الموقع الإلكتروني للمجني عليها أي أن الاختراق هو المرحلة التالية لجريمة الدخول غير المصرح به.

ومما سبق تستنتج الباحثة أن جريمة الاختراق للمواقع الإلكترونية والمنظومة المعلوماتية هي من الجرائم التي لها خصوصية تستقل بها عن بقية الجرائم الأخرى، وهذه الخصوصية تكمن في الهدف من الاختراق وخصوصية الجهات التي تقع عليها جريمة الاختراق والتي تكون في معظمها المواقع الحكومية، وهو ما يعتبر من الخطورة الإجرامية للمخترق حيث أن المواقع الإلكترونية الحكومية تحتوي على العديد من المعلومات الهامة، وعليه توصي الباحثة بأن يقوم المشرع الإماراتي بإضافة مادة إلى المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن الشائعات والجرائم الإلكترونية تبين خصوصية جريمة الاختراق بحيث يتم تمييزها وفق عنصر الخصوصية عن غيرها من الجرائم الإلكترونية الأخرى.
هنا تتمنى الباحثة على المشرع الإماراتي أن يضيف مادة في المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن الشائعات والجرائم الإلكترونية تبين ماهية الاختراق ودوافعه لأن ما ورد في القانون فيما يخص الاختراق يبين أن الاختراق ليس جريمة مستقلة بل هو فعل سابق لجريمة القرصنة أو الإتلاف المعلوماتي ما يتسبب بالخلط بين تلك الأفعال. وتقترح الباحثة أن يكون تعريف الاختراق:" الهجوم الإلكتروني الواقع على منظومة معلوماتية بهدف الدخول غير المرخص به أو المخالف لأحكام الترخيص أو الدخول بطريقة غير مشروعة أو البقاء بصورة غير مشروعة في نظام معلوماتي أو حاسب آلي أو نظام تشغيل جهاز أو آلة أو مركبة أو شبكة معلوماتية وما في

---

[١٦] عمر محمد أبو بكر يونس: المرجع السابق، ، ص٣٢٧.
[١٧] محكمة التمييز - الأحكام الجزائية - الطعن رقم ١٢٨١ لسنة ٢٠١٩ قضائية - الدائرة الجزائية - بتاريخ ٢٠٢١-٠١-٢٤

حكمها" كما تتمنى الباحثة على المشرع الإماراتي أن يضع جريمة الاختراق المعلوماتي وحدها كجريمة مستقلة عن باقي الجرائم، كون ما ورد في القانون يخلط بين الاختراق والبقاء غير المشروع، كما تقترح الباحثة نصاً لهذه المادة على النحو الآتي:" الاختراق هو الهجوم الذي يتم خلاله الدخول للمنظومة المعلوماتية ويتسبب بالنتائج التالية: "الإتلاف" و"التدمير" و"التخريب" و "محو البرامج والبيانات" و"التشويه" و"مسح البرامج والبيانات" و"إيقاف" أو "حذف" أو أي سلوك آخر يجعل البيانات أو المعلومات أو البرامج والمحررات المعلوماتية غير صالحة للاستعمال كلياً أو جزئياً. "

وتتمنى الباحثة على المشرع الإماراتي أن يفرق بين جريمة الاختراق وجريمة الدخول غير المشروع حيث أن الدخول غير المشروع له فعل واحد هو الولوج للمنظومة المعلوماتية، بينما الاختراق قد يكون عن طريق عدة أفعال منها الهاكرز والهجوم السيبراني حتى وإن كان محل الجريمة واحداً في الاختراق والدخول غير المشروع.

كما ان الاختراق هو المرحلة التالية للدخول غير المشروع للمنظومة المعلوماتية الحكومية، ولا يمكن أن يكون الاختراق هو ذاته الدخول غير المشروع.

المبحث الثاني

أركان جريمة اختراق المواقع الإلكترونية الحكومية

تمهيد وتقسيم:

يتطلب المشرع الإماراتي توافر الركن المادي والركن المعنوي لتجريم اختراق الأنظمة الإلكترونية الحكومية، حيث أن الركن المادي يتمثل في السلوك الإجرامي والسببية والركن المعنوي يتمثل بتوافر القصد الجنائي القائم على العلم والإرادة **وعليه** نتناول في هذا المبحث أركان جريمة اختراق المواقع الإلكترونية الحكومية من خلال المطالب التالية:

- **المطلب الأول: الركن المادي اختراق المواقع الإلكترونية الحكومية**
- **المطلب الثاني: الركن المعنوي اختراق المواقع الإلكترونية الحكومية**

المطلب الأول

الركن المادي في جريمة اختراق المواقع الإلكترونية الحكومية

يقصد بالركن المادي: النشاط الذي يؤدي إلى وقوع النتيجة الجرمية مع ضرورة توفر العلاقة السببية بين الفعل والنتيجة[١٨]

لتتكون الجريمة لابد من ارتكاب فعل مادي محسوس (أو امتناع عن إتيان فعل) يعاقب عليه القانون، فالجريمة ليست مجرد وجود نية جرمية، إذ لا بد لهذه النية من أن تتجسد في كيان مادي محسوس، هذا السلوك المادي المحسوس الذي ينص عليه القانون هو ما يعرف بالركن المادي للجريمة، والذي

[١٨] محمد الجبور: الوسيط في قانون العقوبات، القسم العام، الطبعة الأولى، دار وائل، عمان، ٢٠١٢م، ص٥١.

يشكل شرطاً أساسياً للبدء في عملية البحث عن توافر الجريمة من عدمه إن ضرورة أن يكون هناك تجسيد خارجي لما يدور في الأذهان من رغبات وأفكار جرمية له ما يبرره من جهة صعوبة الغور في أعماق النفس البشرية لإثبات حالة نفسية مجردة، ومن جهة أخرى فإن مجرد الرغبات والنوايا الدفينة التي لا تحمل اعتداء ولا تنتج ضرراً للغير لا مبرر لبحثها وترتيب العقاب عليها[١٩].

ولإتمام الركن المادي لا بد من توافر عناصر ثلاثة وهي:

- سلوك جرمي.
- نتيجة جرمية.
- علاقة سببية بينهما.

أولاً: السلوك الجرمي

ذكرنا أن نقطة البدء في البحث عن الجريمة ومعاقبة فاعليها تكون بإظهار النوايا والرغبات إلى حيز الواقع المادي المحسوس بإتيان الفاعل سلوكاً يشكل خرقاً لأمر المشرع بصورة سلبية أو إيجابية. هذا السلوك الجرمي لا يوجد في الواقع العملي بصورة واحدة، بل بتدافع بعدة لعلاج لكل منها ما يميزه، فقد يوجد السلوك الجرمي يفعل إيجابي كإطلاق النار على أحد الأشخاص وقتله، أو سرقة بيت، إذ يفترض في هذه الصورة الإيجابية تحريك الجاني لعضو من أعضائه بشكل إرادي بغية إحداث نتيجة معينة في الواقع، سواءً أكانت هذه الحركة على شكل حركة واحدة كالقتل بطعنة سكين واحدة مثلاً، أو قد يكون السلوك الجرمي الإيجابي مجموعة من الحركات[٢٠]

يقوم السلوك الجرمي أو النشاط المتعلق بالجرائم الإلكترونية على القيام بأوامر تعطى إلى أجهزة الحواسيب أو الهواتف النقالة أو أجهزة تكنولوجيا المعلومات على اختلاف أنواعها من خلال حركات الأيدي أو من خلال الصوت، وذلك بإدخال بعض المعلومات الإلكترونية والبيانات على جهاز الحاسوب أو الشبكة الإلكترونية، وقد عرف المشرع الإماراتي البيانات الإلكترونية في المادة الأولى من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن الشائعات والجرائم الإلكترونية بأنها:" البيانات أو المعلومات: مجموعة منظمة أو غير منظمة من المعطيات، أو الوقائع أو المفاهيم أو التعليمات أو المشاهدات أو القياسات تكون على شكل أرقام أو حروف أو كلمات أو رموز أو صور أو فيديوهات أو إشارات أو أصوات أو خرائط أو أي شكل آخر، يتم تفسيرها أو تبادلها أو معالجتها، عن طريق الأفراد أو الحواسيب، والتي ينتج بعد معالجتها أو تداولها ما يطلق عليه مصطلح معلومات. البيانات والمعلومات الحكومية: البيانات أو المعلومات الإلكترونية غير المتاحة للكافة، والخاصة أو العائدة إلى إحدى مؤسسات الدولة. البيانات والمعلومات الشخصية: المعلومات أو البيانات الخاصة بالأشخاص الطبيعيين متى كانت مرتبطة بحياتهم الخاصة أو تحدد هويتهم أو يمكن من خلال ربط هذه المعلومات والبيانات بطريقة الشخص مباشرة أو غير مباشرة تحديد

---

[١٩] د. عبد الغني قاسم مثنى الشعيبي، شرح قانون الجرائم والعقوبات لدولة الإمارات العربية المتحدة الصادر بمرسوم بقانون اتحادي رقم (٣١) لسنة ٢٠٢١، القسم العام، النظرية العامة للجريمة والنظرية العامة للجزاء الجنائي، مكتبة دار الحافظ، الإمارات العربية المتحدة، ٢٠٢٢ م، ص (٣٧٤ –

[٢٠] دكتور خالد سامي السيد : الأمن القومي الإلكتروني وجرائم المعلومات ـــ دار النهضة العربية – القاهرة – مصر – الطبعة الأولى – ٢٠٢١ – ص٣٠

ومعرفة هوية الشخص. المعلومات والبيانات السرية: أي معلومات أو بيانات غير مصرح للغير بالاطلاع عليها أو بإفشائها إلا بإذن مسبق يملك هذا الإذن."

كما عرف المشرع الإماراتي تكنولوجيا المعلومات في المادة الأولى من المرسم بقانون اتحادي بانها: وسيلة تقنية: أي أداة إلكترونية مغناطيسية، بصرية، كهروكيميائية، أو أي أداة أخرى تستخدم لمعالجة البيانات الإلكترونية وأداء العمليات المنطقية والحسابية، أو الوظائف التخزينية، ويشمل أي وسيلة موصلة أو مرتبطة بشكل مباشر أو غير مباشرة، تتيح لهذه الوسيلة تخزين المعلومات الإلكترونية أو إيصالها للآخرين."

ويلاحظ مما سبق ذكره أن وسائل تكنولوجيا المعلومات تتنوع وتتشكل حسب تطور التكنولوجيا المستمر، حيث حاول المشرع الإماراتي أن يشمل وسائل تكنولوجيا المعلومات كافة، والتي يمكن أن تكون وسيلة أو محلاً لارتكاب الجريمة الإلكترونية.

ونستخلص أن السلوك في الجريمة الإلكترونية غالباً ما يكون إيجابياً بحيث يبادر الشخص الجاني إلى القيام بنشاط يتمثل بإدخال بعض البيانات أو المعلومات والتي تؤدي به إلى إتمام السلوك المادي بمجرد القيام بالأوامر الصوتية والكتابية ووصوله إلى المجني عليه، أو إرسال بعض الصور أو الكتابات أو التسجيلات الصوتية والمرئية إلى بريد الضحية أو (الواتس أب)، أو (الماسنجر)، أو من خلال أي وسيلة إلكترونية أخرى، أو قيام الجاني بإدخال بيانات من خلال وسائل التكنولوجيا المعلومات تهدف إلى السرقة الإلكترونية أو تعطيل البرامج، أو استغلال الأطفال أو التهديد، أو الاختراق لبريد الجاني والوصول إلى أجهزة حواسيب أو مواقع إلكترونية بطريقة غير مشروعة وقد يكون من صور السلوك أيضاً إدخال البيانات الإلكترونية بهدف الحذف، أو النسخ، أو اللصق، أو تعديل، أو قص بيانات، أو معلومات إلكترونية أخرى، إضافة إلى الكثير من الصور الجرمية.

وهنا يمكن الرجوع إلى المادة الأولى من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ والتي تتحدث عن شكل السلوك الذي يتعلق بمعالجة البيانات حيث عرف المشرع في المادة الأولى معالجة البيانات أنها ": معالجة البيانات أو المعلومات: إجراء أو تنفيذ عملية أو مجموعة عمليات على البيانات أو المعلومات، سواء تعلقت بأشخاص طبيعية أو اعتبارية، بما في ذلك جمع واستلام وتسجيل وتخزين وتعديل ونقل واسترجاع ومحو تلك المعلومات."

ومن هذه المادة يتبين أن السلوك الإجرامي في جريمة الاختراق يتمثل في استخدام الجاني لبرمجيات أخرى قادرة على فك الشيفرات الخاصة بالموقع الحكومي محل الاختراق.
وهذا ما أكدته محكمة تمييز دبي، بخصوص جريمة الاختراق حيث جاء في حكم لها:" ..وكان الحكم المطعون فيه وفى حدود السلطة التقديرية في التفسير والتكييف قد أورد في أسبابه أن الغرض غير المشروع على إطلاق عبارة النص يشمل كل فعل أو امتناع عن فعل تجرمه القوانين أو اللوائح ***وأن ما قام به المتهم باعترافه من اختراقه لشبكة الاتصالات الإنترنت التابعة لمؤسسة الإمارات مستخدماً برامج للبحث عن الثغرات واستطاع بذلك الحصول على كلمات السر لبعض المواقع المحظورة على غير موظفي المؤسسة الدخول إليها وقام بفك شفرة بعض الأجهزة ونسخ بعض الملفات وهو يعلم بحظر ذلك لغير موظفي المؤسسة المرخص لهم بذلك كما قام بفك رسائل البريد الإلكتروني لبعض الموظفين ونقلها إلى جهاز الحاسب الآلي الخاص به مما يشكل استغلالاً للشبكة لغرض غير مشروع*** يوقعه تحت طائلة العقاب وهي أسباب سائغة تتفق وصحيح القانون وتتوافر بها كافة الأركان القانونية للتهمة الأولى المسندة إلى الطاعن مما يكون معه منعه في هذا الخصوص

غير سديد لما كان ذلك وكانت خدمة الإنترنت تدخل ضمن الخدمات التي تقدمها مؤسسة الاتصالات وتخضع لأحكام القانون رقم ١/٩١ الخاص بمؤسسة الاتصالات فإن ذلك لا يتعارض مع عدم صدور تشريع خاص بخدمات الإنترنت ويكون منعي الطاعن في هذا الصدد غير مقبول."[٢٠]
ومما ورد في هذا الحكم يتضح أن المحكمة قد بينت السلوك الإجرامي في جريمة الاختراق ووسيلة ارتكاب الجريمة وهي استخدام برامج إلكترونية قادرة على فك الشيفرات في أحد المواقع الحكومة عن طريق استغلال الجاني لبعض الثغرات في النظام الأمني للموقع الإلكتروني للجهة الحكومية محل الاختراق، كما أنها بينت الدوافع التي تمثل الركن المعنوي في هذه الجريمة وهي نقل الملفات والمعلومات ونسخا واستخدامها لغرض غير مشروع، وبالتالي يمكن التأكيد على أن المشرع الإماراتي يعتد بالسلوك الإجرامي في جريمة الاختراق.
بينما تنص المادة (١٧) من القانون المصري على أنه:" يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل أو عدل مسار أو ألغى كلياً أو جزئياً، متعمداً وبدون وجه حق البرامج والبيانات أو المعلومات المخزنة أو المعالجة أو المولدة أو المخلقة على أي نظام معلوماتي وما في حكمه، أيا كانت الوسيلة التي استخدمت في الجريمة."

ومن هذا النص يتضح أن المشرع المصري قد اعتبر الاختراق فعل سابق لجريمة الإتلاف والتعطيل، وبالتالي التأثير على النظام المعلوماتي، وهنا تثور مشكلة خاصة بهذه المادة هي ـأن المشرع المصري لم ينص على الاختراق بشكل صريح، بل اكتفى بعبارة أية وسيلة كانت، وهي ما يمكن أن تنطبق على وسيلة الاختراق، حيث يعتبر الاختراق مقدمة لجريمة الإتلاف أو تحضيراً لها.

كما تنص المادة الأولى من القانون المصري على أنه:" الاختراق: الدخول غير المرخص به أو المخالف لأحكام الترخيص، أو الدخول بأي طريقة غير مشروعة إلى نظام معلوماتي أو حاسب آلي أو شبكة معلوماتية وما في حكمها."

وهنا يتضح لنا من هذه المادة أن كلاً من المشرعين الإماراتي والمصري يعتبران أن الاختراق هو نفسه الدخل غير المشروع للمنظومة المعلوماتية الحكومية، ولكن الصحيح هو أن الاختراق فعل منفصل عن الدخول غير المشروع، أو من الممكن أن يكون الاختراق فعلاً ممهداً له.

ويلاحظ أن كل ما سبق يعتبر أفعالاً تشكل سلوكاً ونشاطاً إيجابياً، بمعنى أن هذا السلوك الوارد ذكره هو السلوك الأساسي الذي يشكل الركن المادي في الجريمة الإلكترونية، كذلك يلاحظ أن المشرع الإماراتي اعترف بشرعية النظام الإلكتروني وبوسائل تكنولوجيا المعلومات وبالتطبيقات والمواقع الإلكترونية واعتبرها مسرحاً معترفاً به لقيام الجريمة، حيث عرف المشرع الإماراتي في المادة الأولى في القانون الإماراتي المذكور التطبيق الإلكتروني على أنه: ام المعلومات الإلكتروني: برنامج معلوماتي أو مجموعة البرامج المعلوماتية المعدة لمعالجة أو إدارة أو تخزين المعلومات الإلكترونية القابلة لتنفيذ التعليمات أو الأوامر بوسائل تقنية المعلومات، ويشمل التطبيقات أو ما في حكمها."

---

[٢٠] محكمة التمييز - الأحكام الجزائية - الطعن رقم ٢٣٠ لسنة ٢٠٠١ قضائية - الدائرة الجزائية - بتاريخ ٢٠٠١-١٢-٠٨ مكتب فني ١٢ رقم الجزء ١ رقم الصفحة ١٢٦٦ [رفض] رقم القاعدة ٥٧

وبالتالي يتصور أن يكون هذا البرنامج الإلكتروني[٢١] وسيلة إلكترونية من أجل الدخول غير المشروع على مواقع الإنترنت أو اختراق أنظمة إلكترونية، وقد يكون هذا التطبيق أو البرنامج محلاً لارتكاب الجريمة من خلال تعرضه للسرقة أو التخريب أو التعديل أو الحذف، حيث اعترف المشرع الإماراتي بهذه البرامج والتطبيقات ووفر لها الحماية القانونية.

ومن الأحكام القضائية للمحكمة الاتحادية العليا بخصوص جريمة الاختراق الإلكتروني عبر الدخول غير المشروع للمواقع الحكومية :" ولما كان ذلك وكانت مدونات الحكم المطعون فيه والمؤيد للحكم المستأنف والمكمل له يكشف أن كلا الحكمين قد ألم بظروف الدعوى وملابساتها ومحص أدلة الثبوت فيها وأفصح عن عدم اطمئنانه إليها وحيث ثبت للمحكمة أن ***المطعون ضده الأول مشترك في خدمة الإنترنت بالاتصالات وقدم فاتورة سداد خدمة الإنترنت صادرة عن هيئة الاتصالات وان دخوله لهذه الشبكة مشروع , ولم يثبت لديها أن المتهمين كانا يتجران في المكالمات الدولية*** ثم انتهى إلى القضاء ببراءتهما مما اسند إليهما , ومن ثم فإن ما تثيره الطاعنة في هذا النعي لا يعدو أن يكون جدل موضوعي حول تقدير المحكمة للأدلة القائمة في الدعوى وهو ما لا يقبل إثارته أمام محكمة النقض[٢٢]."

ومن هذا الحكم يتضح أن السلوك الإجرامي في جريمة الاختراق وفق ما جاءت به المحكمة هو دخول الجاني إلى موقع إلكتروني حكومي بشكل غير مشروع والتلاعب بالبيانات بهدف التزوير للفواتير الإلكترونية، وبالتالي فإن السلوك الذي قام به الجاني هو سلوك إيجابي يمثل عنصر ها في الركن المادي لجريمة الاختراق.

وقد يتم استخدام كلمة السر كنشاط من الأنشطة غير المشروعة والتي تستخدم لإتمام النشاط الجرمي في الجريمة الإلكترونية، حيث عرف المشرع الإماراتي في المادة الأولى من القانون الإماراتي المعلومات السرية بأنها:" المعلومات والبيانات السرية: أي معلومات أو بيانات غير مصرح للغير بالاطلاع عليها أو بإفشائها إلا بإذن مسبق يملك هذا الإذن."

الصورة الأولى: السلوك الإيجابي

والذي يتطلب مجهوداً عقلياً وبدنياً بسيطاً يتمثل في العالم الخارجي من حركات تتمثل بإدخال بيانات إلكترونية يأتيها الجاني بهدف الاعتداء على المصلحة التي يحميها الشارع، ومثال ذلك في الجرائم الإلكترونية كل الأفعال التي يرتكبها الجاني في التلاعب في بيانات الحاسوب بهدف إتلاف البيانات أو سرقتها أو نسخها، وكذلك السلوك الإجرامي الإيجابي كاستخدام الجاني وسائل الاتصال بشكل غير قانوني، كأن يقوم باختراق شبكات الاتصال أو أن يقوم الجاني باختراق شبكات الاتصال ويحصل على بيانات الشركات الخاصة ويقوم بنشرها، أو يهدد أصحابها باستخدامها بشكل غير مشروع[٢٣].

---

[٢١] عرفت المادة الثانية من الاتفاقية العربية جرائم تقنية المعلومات لعام ٢٠١٠م، (البرنامج المعلوماتي) على أنها "مجموعة من التعليمات والأوامر. قابلة للتنفيذ باستخدام تقنية المعلومات ومعدة لإنجاز مهمة ما"، كما عرفت النظام المعلوماتي على أنه "مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات".

[٢٢] المحكمة الإتحادية العليا - الأحكام الجزائية - الطعن رقم ١٨٥ لسنة ٢٠١١ قضائية بتاريخ ٢٠١١-٠٦-٢١ [رفض]

[٢٣] عبد الفتاح بيومي حجازي: الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، المركز القومي للإصدارات القانونية، مصر، ٢٠١١م، ص٢٦٦.

وفي حكم آخر للمحكمة الاتحادية العليا جاء فيه:" ارتكبوا جميعا: ١- تزويرا في صورة محرر عرفي - عقد الإيجار رقم ..... المبين بالأوراق - ***<u>عن طريق إدخال تغيير على المحرر الموجود بحذف البيانات السابقة وإدراج بيانات أخرى وكان من شأنه إحداث ضرر بصاحبه وبنية استعماله كمحرر صحيح على النحو المبين بالأوراق</u>***."[٢٤]

ومن هذا الحكم يتضح أن جريمة التزوير قد تمت عن طريق الاختراق الإلكتروني لأحد الأنظمة الإلكترونية الحكومية، وبالتالي فإن السلوك الإجرامي محقق بفعل إيجابي يسبق عملية التزوير ويعتبر تمهيداً لها.

الصورة الثانية: السلوك السلبي

وهي الامتناع عن إتيان أمر بوجه مشروع، فمن الممكن ارتكاب جريمة بالكف عن عمل معين كان من الواجب مباشرته، وهذا الامتناع عن قاعدة آمرة فرضها المشرع، مثل امتناع المنقذ البحري من إنقاذ غريق كان بإمكانه إنقاذه، أما عن صور الامتناع في الجرائم الإلكترونية، فهي مع اختلاف الفقهاء متوافرة، ومن الممكن حدوثها، مثل امتناع موظف أمن عن حماية بيانات الشركة ومعلوماتها التي يعمل بها، أو عدم الإبلاغ عن جريمة للحفاظ على حقوق الآخرين وخصوصيتهم، أو عدم التدخل للحفاظ على أسرار الدولة في الجرائم التي تمس أمن الدول[٢٥].

وبالرجوع إلى المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن الشائعات والجرائم الإلكترونية نلاحظ أن النشاط السلبي كصورة من صور النشاط الجرمي أشار إليه المشرع الإماراتي في نص المادة (٥٣) التي تنص على أنه:" يعاقب بغرامة لا تقل عن (٣٠٠,٠٠٠) ثلاثمائة ألف درهم ولا تزيد على (١٠,٠٠٠,٠٠٠) عشرة ملايين درهم كل من أستخدم موقع أو حساب إلكتروني في ارتكاب أيا من الأفعال الآتية:

١) خزن أو أتاح أو نشر محتوى غير قانوني، ولم يبادر بإزالته أو منع الدخول إلى هذا المحتوى خلال المدة المحددة في الأوامر الصادرة إليه والمنصوص عليها في هذا المرسوم بقانون.
٢) امتنع عن الامتثال كليا أو جزئيا لإحدى الأوامر التي صدرت إليه والمنصوص عليها في هذا المرسوم بقانون، دون عذر مقبول".

ومن نص هذه المادة يتضح أن المشرع الإماراتي يعتبر أن السلوك السلبي في جريمة اختراق المواقع الإلكترونية الحكومية يتمثل في الامتناع عن الامتثال للأوامر التي تصدرها الجهات المختصة لمن يتعامل مع المنظومة المعلوماتية الحكومية.

بينما تنص المادة (٢٢) من القانون المصري على أنه: يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من حاز أو أحرز أو جلب أو باع أو أتاح أو صنع أو أنتج أو استورد أو صدر أو تداول بأي صورة من صور التداول، أي أجهزة أو معدات أو أدوات أو برامج مصممة أو مطورة أو محورة أو أكواد مرور أو شفرات أو رموز أو أي بيانات مماثلة، بدون تصريح من الجهاز أو مسوغ من الواقع أو القانون، وثبت أن ذلك السلوك كان بغرض استخدام أي منها في ارتكاب أو تسهيل ارتكاب

---

[٢٤] المحكمة الإتحادية العليا - الأحكام الجزائية - الطعن رقم ١٢٨٥ لسنة ٢٠٢٠ قضائية بتاريخ ٢٠٢١-٠٣-٠١ [رفض الطعن]

[٢٥] إبراهيم محمود اللبيدي: السلوك الإجرامي في جرائم الإنترنت، مركز الإعلام الأمني، القاهرة، ص٢٥.

أية جريمة من الجرائم المنصوص عليها في هذا القانون، أو إخفاء آثارها أو أدلتها أو ثبت ذلك الاستخدام أو التسهيل أو الإخفاء."

ومن هذه المادة يتضح أن المشرع المصري يعتبر أن النشاط السلبي على سبيل المثال، يتصور في عدم اتخاذ الشركة المزودة بالإنترنت لبعض الوسائل التي توفر الأمن المعلوماتي للمستخدم بصورة عمدية، أو تعمد بعض مسؤولي الشبكات الإلكترونية (الآدمن)، إلى عدم القيام بواجباته أو عدم توفير الحماية لجهاز الحاسوب المطلوب توفير حماية له من قبل المسؤول عن الشبكة الإلكترونية (الآدمن)، مع الإشارة أيضاً إلى أن المشرع الإماراتي لم يشر بصورة واضحة إلى عقوبة الأشخاص الذين يرتكبون الجريمة الإلكترونية بصورة النشاط السلبي في القرار بقانون المذكور.

ثانياً: النتيجة الجرمية

المقصود بالنتيجة الجرمية الأثر الذي يحدثه السلوك الجرمي والذي يرتب عليه المشرع أحكاماً قانونية[٢٦].

وللنتيجة وفقاً لما تقدم معنيان: الأول مادية وهو إحداث أثر ناتج عن السلوك المرتكب من الفاعل، والثاني معنى قانوني قوامه التأثير على مصلحة يقرر لها المشرع حماية محددة.[٢٧]

تتحقق النتيجة الجرمية في الجريمة الإلكترونية من خلال وقوع نشاط في محل الجريمة سواءً كانت الجريمة واقعة على الأفراد من خلال استخدام الوسائل الإلكترونية، أو على وسائل التكنولوجيا المختلفة، حيث ينشأ عن ذلك أثر مادي وقانوني، وبالتالي يشكل اعتداء على حق يحميه القانون، فالنشاط المتمثل بالاختراق أو النسخ أو الحذف أو التعديل وغيرها من الأنشطة غير المشروعة، والتي تقع على البيانات والمعلومات المخزنة على جهاز الحاسوب، وعلى الشبكة الإلكترونية، أو على أي وسيلة تكنولوجيا المعلومات، وتكون محمية بموجب أحكام القانون، تجعل من النتيجة قائمة بمجرد قيام النشاط الجرمي، وحتى ولم يقع الضرر المادي بشكل مباشر، فالجرائم الإلكترونية تعتبر من جرائم الخطر التي تقع بمجرد استكمال النشاط المادي.[٢٨]

فالنتيجة الجرمية تتحقق بمجرد قيام الشخص بالدخول غير المشروع أو الحذف أو الإتلاف وغيرها، من الأنشطة غير المشروعة، وكان لا يملك الصفة القانونية للدخول غير المشروع، أو للحذف، أو التعديل، أو الإتلاف، أو غيرها من الأنشطة، أو أن صفته كانت قائمة وكان له صلاحيات للدخول أو التعديل ولكنها انتهت كالموظف الذي يستقيل من عمله، وبالتالي فهو غير مسؤول عن البيانات والمعلومات الإلكترونية، أو كالموظف الذي يتجاوز الحد المسموح له في التعديل أو الحذف أو البقاء على النظام.[٢٩]

---

[٢٦] خالد حربي السعدي: جريمة إتلاف برامج ومعلومات الحاسب الآلي في التشريعين الكويتي والمقارن ، دار النهضة العربية، القاهرة، ٢٠١٢، ص ٣٨.

[٢٧] الدكتور عمار عباس الحسيني : جريمة الإتلاف المعلوماتي ـــ مكتبة زين الحقوقية الأدبية – بيروت – لبنان – الطبعة الأولى – ٢٠١٩م – ص٤٩

[٢٨] أمير فرج يوسف، جرائم تقنية المعلومات بدول الخليج العربي والجهود الدولية والمحلية لمكافحة جرائم الإنترنت والحاسوب الإلكترونية في دول الخليج العربي، دار الكتب والدراسات العربية، الطبعة الأولى ٢٠١٥م، ص٢١٨

[٢٩] دكتور خالد سامي السيد : الأمن القومي الإلكتروني وجرائم المعلومات ـــ دار النهضة العربية – القاهرة – مصر – الطبعة الأولى – ٢٠٢١ – ص٥٤

وفي جريمة الاختراق بين المشرع الإماراتي النتيجة الجريمة في نص الفقرة الثالثة من المادة (٣) من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن الشائعات والجرائم الإلكترونية التي تنص على أنه:" ٣. وتكون العقوبة السجن المؤقت مدة لا تقل عن (٧) سنوات والغرامة التي لا تقل عن (٢٥٠,٠٠٠) مائتين وخمسين ألف درهم ولا تزيد على (١,٥٠٠,٠٠٠) مليون وخمسمائة ألف درهم، إذا كان الاختراق بغرض الحصول على البيانات أو المعلومات الخاصة بتلك الجهات المنصوص عليها بالفقرة الأولى من هذه المادة."

يقصد بالنتيجة الإجرامية الأثر القانوني المترتب على السلوك الإجرامي والذي يرتب عليه المشرع أحكام قانونية.

ومن هذه المادة يتضح أن المشرع الإماراتي قد بين بشكل واضح النتيجة الإجرامية في جريمة اختراق المواقع الحكومية وهي بغرض الوصول إلى البيانات والمعلومات للحصول عليها.

فيما تنص المادة (٢٢) من القانون المصري على أنه:" يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من حاز أو أحرز أو جلب أو باع أو أتاح أو صنع أو أنتج أو استورد أو صدر أو تداول بأي صورة من صور التداول، أي أجهزة أو معدات أو أدوات أو برامج مصممة أو مطورة أو محورة أو أكواد مرور أو شفرات أو رموز أو أي بيانات مماثلة، بدون تصريح من الجهاز أو مسوغ من الواقع أو القانون، وثبت أن ذلك السلوك كان بغرض استخدام أي منها في ارتكاب أو تسهيل ارتكاب أية جريمة من الجرائم المنصوص عليها في هذا القانون، أو إخفاء آثارها أو أدلتها أو ثبت ذلك الاستخدام أو التسهيل أو الإخفاء."

ومن هذه المادة يتضح أن المشرع المصري لم يشير للنتيجة الإجرامية لجريمة الاختراق ولكنه نص على بعض الأفعال التي يفهم معها انها تعبر بطريقة أو بأخرى عن النتيجة الإجرامية في جريمة الاختراق.

وبالتالي في نطاق الجرائم الإلكترونية فإن العلاقة السببية أساسية لقيام جميع أنواع الجرائم الإلكترونية، فهي عنصر أساسي من عناصر الركن المادي لأي جريمة إلكترونية، وتقوم العلاقة السببية في الجرائم الإلكترونية على البحث في الصلة بين مرتكب الجريمة والفعل الذي ارتكبه من خلال الوسيلة التكنولوجية المستخدمة في ارتكاب الجريمة والنتيجة الجرمية، وهنا نرى أن نظرية السببية المباشرة والتي تقوم على التمييز بين الجرائم المقصودة والجرائم غير المقصودة، حيث يجب أن تتوافر علاقة السببية المباشرة بين مرتكب الجريمة وبين الوسيلة التكنولوجية المستخدمة في ارتكاب الجريمة الإلكترونية والنشاط الجرمي هي الأساس لبيان رابطة السببية بين السلوك والنتيجة الجرمية، حيث يعتبر السلوك الجرمي العنصر الأساسي في بيان الرابط السببية بسبب كون كثير من الجرائم الإلكترونية من جرائم الخطر والتي تقع بمجرد قيام السلوك الجرمي[٣٠].

المطلب الثاني

الركن المعنوي اختراق المواقع الإلكترونية الحكومية

[٣٠] الدكتور محمود رجب فتح الله: الوسيط في الجرائم المعلوماتية دار الجامعة الجديدة الطبعة الأولى، سنة ٢٠١٨، ص ١ وما بعدها.

إن هذه الجريمة من الجرائم العمدية التي لا يكفي فيها مجرد تحقق الركن المادي، وإنما يلزم أيضاً أن يتوافر لها الركن المعنوي، الذي يمثل الجانب الشخصي لها باعتباره يجسد العلاقة النفسية بين السلوك الإجرامي ومرتكبه، حتى يمكن إسناد الجريمة إليه. فالجريمة ليست ظاهرة مادية خالصة، قوامها الفعل وآثاره، ولكنها كذلك كيان نفسي. وقد استقر هذا المبدأ في التشريعات الحديثة الذي يقضي بأن ماديات الجريمة لا تنشئ مسؤولية ولا تستوجب عقاباً ما لم تتوافر إلى جانبها العناصر النفسية التي يتطلبها كيان الجريمة. وتجتمع هذه العناصر في ركن يختص بها ويحمل اسم "الركن المعنوي"[٣١].

والركن المعنوي الذي يتكون من العناصر العقلية والنفسية التي يعينها المشرع في النموذج القانوني للجريمة، ما هو إلا جزء من كل نسميه معنويات الجريمة التي تتكون من كل ما له ارتباط بالحالة العقلية والنفسية للجاني، وتتضمن بالإضافة للركن المعنوي، شروط المسؤولية الجزائية (الإدراك وحرية الاختيار).

تنص المادة /٣٩/ من قانون الجرائم والعقوبات الإماراتي على أن الركن المعنوي يتكون من "العمد أو الخطأ" وبذلك يظهر الركن المعنوي في صورتين: القصد الجنائي (العمد) والخطأ.

الصورة الأولى: وتكون الإرادة فيها متجهة إلى عناصر الركن المادي للجريمة بكاملها، ومسيطرة عليها، وقادرة على توجيهها نحو الفعل والنتيجة بآن واحد، وهذا ما يسمى (القصد الإجرامي) وبه تكون الجريمة عمدية.

الصورة الثانية: وتكون الإرادة فيها مسيطرة على جزء من الركن المادي للجريمة فقط (وهو السلوك)، وغير مسيطرة على الجزء الآخر (وهو النتيجة) وهذا ما يسمى (بالخطأ) وبه تكون الجريمة غير عمدية.

أولاً: نظرية العلم

تجمل هذه النظرية في أن القصد الجرمي يتمثل في العلم وإرادته، ثم في توقع النتيجة من دون إرادتها. فدور الإرادة إذاً، يقتصر على السيطرة على الفعل من دون النتيجة بينما العلم يشمل تلك النتيجة فضلاً عن كافة الوقائع والظروف الأخرى التي تدخل في النموذج القانوني للجريمة

والعلم بالنتيجة، أي توقعها، هو الأساس المطلوب لتوافر القصد من دون اتجاه الإرادة إلى تحقيقها[٣٢]. لذلك فإن أنصار هذه النظرية يستبعدون من نطاق القصد إرادة النتيجة. ويعلل هؤلاء موقفهم بأن إرادة النتيجة هي أمر غير لازم من الناحية القانونية، فضلاً عن كونه غير صحيح من الناحية المنطقية.

ثانياً: نظرية الإرادة

---

[٣١] -عبد العزيز الحسن: علم النفس في علم الجريمة والجريمة، كل الأطروحة، جامعة روبرت شومان في ستراسبورغ، ١٩٩٨.ص٣٢

[٣٢] الدكتور محمد عبد الله محمد العوا: المسئولية الجنائية الناشئة عن جرائم الأموال عبر الانترنت، رسالة دكتوراه بكلية الحقوق جامعة الاسكندرية، ٢٠١٢، ص ٢٣- ٢٤.

القصد الجرمي لا يقوم بمقتضى هذه النظرية، إلا إذا توافرت للفاعل إرادة الفعل وإرادة النتيجة على حد سواء[٣٣].

ويرى أنصار هذه النظرية أن اخص ما يميز السلوك الإنساني هو كونه متجهاً نحو غاية معينة، يعد وسيلة لتحقيقها، وهي مسألة خارجة عن نطاق الجاني ومترتبة على سلوكه، ولا يكفي للقول بمسؤوليته الجزائية عنها محض توقعه لها، وإنما يجب فضلاً عن هذا أن تتجه إرادته إليها[٣٤].

فالإرادة نشاط نفسي يوجهه صاحبه إلى غاية معينة من دون أن يتطلب ذلك السيطرة على سبيل تحقيق هذه الغاية. فبغير هذا النشاط النفسي المحدد لا تكون في مجال القصد الجنائي، وإنما في مجال الخطأ (الجرائم غير العمدية).

وتجدر الإشارة إلى أنه يلاحظ من النصوص التشريعية أن المشرع الإماراتي يشدد في العقاب في حال كانت الجريمة متعلقة بالأمن الوطني، أو على بيانات، أو مواقع حكومية. وفق ما جاءت به المادة (٣) من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١.

ولكن ماذا لو كانت نية الفاعل الذي قام بالاختراق غير متوجهة نحو النشر أو الحذف أو النسخ للبيانات والمعلومات الإلكترونية، وحدث لسبب خارج عن إرادته حذف بعض المعلومات؟

فهنا وكأننا تصبح أمام جريمة عمدية في حالة الدخول غير المصرح البسيط، أما حذف البيانات وإتلافها ونسخها وغيرها من الصور، يمكن أن تتم بصورة غير عمدية، وبالتالي كان يفضل على المشرع أن يقول في المادة (٣) من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن الشائعات والجرائم الإلكتروني: (إذا قصد الفاعل من الدخول غير المصرح إلغاء بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي، أو حذفها، أو إضافتها، أو إفشاؤها، أو إتلافها، أو تدميرها، أو تغييرها، أو نقلها، أو التقاطها، أو نسخها أو نشرها، أو إعادة نشرها، أو إلحاق ضرر بالمستخدمين أو المستفيدين، أو تغيير الموقع الإلكتروني، أو إلغاؤه، أو تعديل محتوياتها، أو شغل عنوانه، أو تصميماته، أو طريقة استخدامه، أو انتحال شخصية مالكه، أو القائم على إدارته) بمعنى أنه لا يشترط القصد الجنائي الخاص بشكل واضح في المادة (٣) من القانون الإماراتي التي تنص على أنه:"

١) يعاقب بالسجن المؤقت والغرامة التي لا تقل عن (٢٠٠,٠٠٠) مائتي ألف درهم ولا تزيد على (٥٠٠,٠٠٠) خمسمائة ألف درهم، كل من اخترق موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات عائدة لمؤسسات الدولة.
٢) وتكون العقوبة السجن مدة لا تقل عن (٥) خمس سنوات والغرامة التي لا تقل عن (٢٥٠,٠٠٠) مائتين وخمسين ألف درهم ولا تزيد على (١,٥٠٠,٠٠٠) مليون وخمسمائة ألف درهم، إذا ترتب على الاختراق إحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات أو خسارة سريتها أو وقعت الجريمة نتيجة لهجمة إلكترونية.

---

[٣٣] د. عبد العزيز أحمد الحسن، شرح قانون الجرائم والعقوبات الاتحادي لدولة الإمارات العربية المتحدة الصادر بموجب المرسوم بقانون اتحادي رقم ٣١ لسنة ٢٠٢١، الأحكام العامة، الكتاب الأول، النظرية العامة للجريمة، دار النهضة العلمية ٢٠٢٢، ص (١٤١

[٣٤] – د. محمود نجيب حسني – النظرية العامة للقصد الجنائي – مرجع سابق – ص ٣٢.

٣) وتكون العقوبة السجن المؤقت مدة لا تقل عن (٧) سنوات والغرامة التي لا تقل عن (٢٥٠,٠٠٠) مائتين وخمسين ألف درهم ولا تزيد على (١,٥٠٠,٠٠٠) مليون وخمسمائة ألف درهم، إذا كان الاختراق بغرض الحصول على البيانات أو المعلومات الخاصة بتلك الجهات المنصوص عليها بالفقرة الأولى من هذه المادة.

وذلك كشرط القيام الجريمة، ويلي هذه الحالة يعاقب المشرع الإماراتي:" ، إذا ترتب على الاختراق إحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات أو خسارة سريتها أو وقعت الجريمة نتيجة لهجمة إلكترونية."

ومن الأحكام القضائية حول حذف البيانات حكم لمحكمة تمييز دبي:" حيث أن الحكم الابتدائي المؤيد لأسبابه والمعدل بالحكم المطعون فيه قد بين واقعة الدعوى في قوله: "أنه حال عمل المتهم بشركة المجني عليه (.....) كمدير مبيعات ***قام بالدخول على النظام الإلكتروني الخاص بالشركة متجاوزا حدود التصريح الممنوح له بصورة غير مشروعه وترتب على ذلك حذف البيانات والمعلومات الخاصة بالشركة المذكورة وعملائها وإعادة استرجاع تلك البيانات ونسخها كما قام بإفشاء أسرار الشركة وبياناتها بأن استخدم بيانات الشركة ومعلوماتها السرية لمنفعته الشخصية دون إذن من صاحب الشأن وذلك بأن قام بنسخها على قرص صلب خارجي واحتفظ به لنفسه، كما مكن شخص خارجي من الدخول إلى برنامج الشركة والتحكم في جهاز الحاسب الآلي المسلم للمتهم من الشركة والذي عليه كل أسرارها من بيانات العملاء وغيرها من المعلومات***، وقد اعترف المتهم بمحضر تحقيقات النيابة العامة بأن الرسائل الإلكترونية التي قام باسترجاعها بعد حذفها كانت بها جميع بيانات العملاء والزبائن والمعاملات والشركات التي كانت شركته تتعامل معها".[١٠٠]"

ومن هذا الحكم يتضح أن الركن المعنوي في الجريمة يتمثل في علم الجاني بأنه يخترق أحد المواقع الإلكترونية للمجني عليه وبالتالي إرادة الحصول على الوثائق والمعلومات الخاصة بالعملاء بشكل غير مشروع، وهنا يمكن القول بأن المحكمة اعتمدت على وقائع القضية في إثباتها للركن المعنوي لجرمية الاختراق.

أما في القانون المصري تنص المادة (٢٤) على أنه:" يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدا، أو دخل بخطأ غير عمدي وبقى بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه. فإذا نتج عن ذلك الدخول إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي، تكون العقوبة الحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين."

ومن هذه المادة يتضح أن المشرع المصري يتعامل مع جريمة اختراق الأنظمة المعلوماتية بحكم أنها ذاتها جريمة الدخول غير المشروع لمنظومة معلوماتية، ونلاحظ هنا أن المشرع المصري لا

---

[١٠٠] محكمة التمييز - الأحكام الجزائية - الطعن رقم ٥٤٠ لسنة ٢٠١٧ قضائية - الدائرة الجزائية - بتاريخ ٢٠١٧-٠٩-٢٥ مكتب فني ٢٨ رقم الصفحة ٤٦٣ [نقض الحكم والإحالة] رقم القاعدة ٥٨

يفرق بين ما إذا كان الاختراق قد تم عمداً أو انه قد تم عن طريق الخطأ، والسبب في ذلك من وجهة نظر الباحثة أن المشرع المصري يعتد بنتيجة الاختراق أكثر من اعتداده بفعل الاختراق ذاته.

كما تنص المادة (١٥) من القانون المصري على أنه:" يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتي مستخدما حقا مخولا له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول."

ومن هذه المادة يتضح أن المشرع المصري يأخذ بنظرية الإرادة فيما يتعلق بالركن المعنوي لجريمة الاختراق، وخاصة أنه نص على عبارة (مستخدماً حق مخول له) وهو ما يدل على أن الركن المعنوي في جريمة الاختراق يقوم على الإرادة أي الدخول للنظام المعلومات الحكومية استغلالاً لحق منحه القانون للجاني، وهذا الامر ينصرف على الموظف الذي يرتكب جريمة الاختراق.

إلا أن المشرع الإماراتي عاد واشترط القصد الجنائي الخاص في المادة (٣) من القانون بقانون كشرط لقيام التجريم حيث نصت على أنه: إذا كان الاختراق بغرض الحصول على البيانات أو المعلومات الخاصة بتلك الجهات المنصوص عليها بالفقرة الأولى من هذه المادة."

وبالتالي جعل المشرع الإماراتي القصد الجنائي العام المتمثل في الدخول غير المشروع للأنظمة الحاسوبية، ومن ثم اشترط القصد الجنائي الخاص والمتمثل في الحصول على المعلومات بغرض استخدامه بشكل غير مشروع.

لكن ماذا لو تم الاختراق إلى النظام الإلكتروني دون توفر العلم في البداية لدى المستخدم بأن دخوله غير مشروع ولكن بعد فترة زمنية علم المستخدم أن دخوله غير مشروع على النظام أو الشبكة الإلكترونية ولكنه استمر بالدخول؟

أجاب المشرع الإماراتي على هذا التساؤل، حيث أورد أن هذه الجريمة لا تقوم إلا بتوفر العلم لدى المستخدم بأن دخوله غير مشروع، فإذا علم بعد دخوله واستمر بالدخول، فتقوم الجريمة من لحظة علمه بالاختراق بشرط أن يكون استمر بالبقاء على النظام أو الشبكة المعلوماتية، أما إذا قام بالاختراق دون علمه بأن دخوله غير مشروع، وانتهى عمله على النظام أو على الشبكة وبعد انتهاء النشاط، علم أن دخوله كان غير مشروع فلا تقوم الجريمة، لأن الفعل أو النشاط قد انتهى، وهو ما جاء في المادة (٣) من القانون الإماراتي التي تنص على أنه:" كل من اخترق موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات عائدة لمؤسسات الدولة."

وهذا الحكم قريب لما جاءت به المادة (١٨) من القانون المصري التي تنص على أنه:" يعاقب بالحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل أو أبطأ أو اخترق بريدا إلكترونيا أو موقعا أو حسابا خاصا بآحاد الناس. فإذا وقعت الجريمة على بريد إلكتروني أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة، تكون العقوبة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين"

وتجدر الإشارة إلى أن تجاوز المستخدم التصريح الخاص بالدخول أو بالاطلاع على بيانات أخرى أو قام بالمكوث أكثر من المدة المحددة في تصريح الدخول مع علمه بذلك، فإن الجريمة في تلك

الحالة تعتبر قائمة والعلة من ذلك أن المشرع أراد توفير أكبر حماية للأنظمة والشبكات الإلكترونية وللمعلومات المخزنة عليها.

المبحث الثالث

العقوبات والتدابير المقررة لجريمة الاختراق الإلكترونية

تطورت الجريمة السيبرانية مع تطور التكنولوجيا الحديثة، واعتمد المخترقون على مزايا التكنولوجيا الحديثة في تنفيذ عمليات الاختراق التي تشكل هجمات إلكترونية ضد أنظمة المعلومات، وتحديداً استهداف الجهات الحكومية .وتحدث القرصنة الإلكترونية من خلال أحدث التقنيات نفسها، مثل الهجمات التي تستهدف الأنظمة التقنية لذا فإن مجرد اقتحام نظام إلكتروني ليس أمرًا غير قانوني، لكن الاختراق يجعله غير قانوني. حيث يتم الوصول غير المصرح به وغير المصرح به إلى جهاز كمبيوتر عن طريق الوصول إلى المعلومات أو البيانات المخزنة على نظام الكمبيوتر دون موافقة الشخص المسؤول عن النظام. وقد أفرد المشرع الإماراتي العديد من العقوبات لجريمة الاختراق الإلكتروني.

نتناول في هذا المبحث العقوبات والتدابير المقررة لجريمة الاختراق الإلكترونية من خلال المطالب التالية:

- **المطلب الأول: العقوبات الأصلية لجريمة اختراق المواقع الإلكترونية الحكومية**
- **المطلب الثاني: العقوبات التبعية والتكميلية لجريمة اختراق المواقع الإلكترونية الحكومية**
- **المطلب الثالث: ظروف التشديد والتخفيف والإعفاء من العقوبة لجريمة اختراق المواقع الإلكترونية الحكومية**

المطلب الأول

العقوبات الأصلية لجريمة اختراق المواقع الإلكترونية الحكومية

يقصد بالعقوبة الأصلية تلك العقوبة التي فرضها القانون أصلاً لكل من ثبت ارتكابه الجريمة، في الجزاء الأصلي والأساسي المباشر للجريمة، ولا توقع إلا إذا نطق بها القاضي وحدد نوعها ومقدارها، وتكفي وحدها لتحقيق أغراضها[٣٥]. وتتعدد العقوبات الأصلية تبعاً لجسامة الجرائم المرتكبة، فمنها ما يمس حياة الإنسان، ومنها ما يمس حرية المحكوم عليه فيترتب عليها سلبها، ومنها ما يمس الذمة المالية للمحكوم عليه. وقد بين المشرع الإماراتي هذه العقوبات في المواد (٦٧ - ٧٣) من قانون الجرائم والعقوبات الاتحادي.

[٣٥] د. طارق العبدالله: شرح قانون الجرائم والعقوبات الاتحادي، دار النهضة العلمية، القاهرة، ٢٠٢٢، ص ١١٢

وتنقسم العقوبات الأصلية من حيث المصدر التي تستقى منه إلى قسمين: عقوبات شرعية تتمثل في عقوبات الحدود والقصاص والدية، يرجع في تحديد نطاقها، وضوابط فرضها إلى أحكام الشريعة الإسلامية. وعقوبات تعزيرية تتمثل بالإعدام والسجن المؤبد أو المؤقت والحبس والحجز والغرامة تضمنها قانون الجرائم والعقوبات الاتحادي وبين مددها، ومقدارها، وكيفية تطبيقها، وحالات انقضائها.

تنص المادة (٢) من المرسوم بقانون اتحادي رقم (٤٣) لسنة ٢٠٢١ على أنه:"

١) يعاقب بالحبس والغرامة التي لا تقل عن (١٠٠,٠٠٠) مائة ألف درهم ولا تزيد على (٣٠٠,٠٠٠) ثلاثمائة ألف درهم، أو بإحدى هاتين العقوبتين، كل من اخترق موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات.
٢) وتكون العقوبة الحبس مدة لا تقل عن (٦) ستة أشهر والغرامة التي لا تقل عن (١٥٠,٠٠٠) مائة وخمسون ألف درهم ولا تزيد على (٥٠٠,٠٠٠) خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين، إذا ترتب على الاختراق إحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أو الحصول على أي بيانات أو معلومات أو خسارة سريتها.
٣) وتكون العقوبة الحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن (٢٠٠,٠٠٠) مائتي ألف درهم ولا تزيد على (٥٠٠,٠٠٠) خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين، إذا كان الاختراق بغرض الحصول على البيانات أو المعلومات لتحقيق غرض غير مشروع."

ومن خلال ما ورد في هذه المادة ترى الباحثة: أن المشرع الإماراتي قد حدد عدة عقوبات أصلية على جريمة الإختراق الإلكتروني، فمن خلال ما جاءت به الفقرة الأولى من هذه المادة يتضح أن المشرع الإماراتي نص على عقوبة الحبس والغرامة التي لا تقل قيمتها عن (١٠٠ألف درهم) ولا تزيد على (٣٠٠ ألف درهم)، وهنا يمكن القول بأن المشرع الإماراتي أجاز الجمع بين عقوبتين أصليتين هما الحبس والغرامة، كما أنه أجاز للمحكمة أن تحكم إما بالحبس أو بالغرامة وحدها، أي أن المشرع الإماراتي ترك للمحكمة السلطة التقديرية في تقدير اختيار العقوبات الأصلية على جريمة الاختراق، وفق ظروف كل قضية وملابساتها، كما أن العقوبة التي تنص عليها الفقرة الأولى من هذه المادة هي عن نوع واحد من أنواع جريمة الاختراق وهي جريمة (اختراق كل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات.)

أما الفقرة الثانية من هذه المادة فقد بين المشرع الإماراتي خلالها العقوبات الأصلية في جريمة الاختراق ولكن لنوع ثاني من أنواع جرائم الاختراق، والعقوبة الأصلية المقررة في الفقرة الثانية من هذه المادة هي عقوبة (الحبس لمدة لا تقل ستة أشهر) والغرامة التي لا تقل عن (١٥٠ ألف درهم) ولا تزيد على نصف مليون درهم، وكما فعل المشرع الإماراتي في الفقرة الأولى من هذه المادة فقد نص على السلطة التقديرية للمحكمة بأن تحكم بالحبس أو الغرامة أو الحبس والغرامة وفق حيثيات كل قضية وملابساتها، وهنا تلاحظ الباحثة أن المشرع الإماراتي قد شدد العقوبة على الاختراق في الفقرة الثانية من هذه المادة عما هو الحال عليه في المادة السابقة، وخاصة من حيث أنه حدد مدة الحبس بأن لا تقل عن ستة أشهر وحدد كذلك رفع الحد الأعلى والحد الأدنى للغرامة،

والعبرة في ذلك أن المشرع الإماراتي يتدرج في تشديد العقوبات الأصلية على جريمة الاختراق، حيث أن التشديد هنا كان لنتيجة جريمة الاختراق حيث أن المشرع الإماراتي بين في نص الفقرة الثانية من هذه المادة أن العقوبة المقررة هي للنتائج التي تنجم عن الاختراق وبينها في نهاية الفقرة الثانية من المادة بأنها:" إذا ترتب على الاختراق إحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أو الحصول على أي بيانات أو معلومات أو خسارة سريتها."

ومن خلال الفقرة الثالثة من هذه المادة يتضح أن المشرع الإماراتي اتبع أيضاً أسلوب التدرج في تشديد عقوبة جريمة الاختراق، حيث تلاحظ الباحثة أن المشرع الإماراتي نص في الفقرة الثالثة من هذه المادة على عقوبة أشد من سابقتها التي وردت في الفقرة الثانية من هذه المادة وهي (الحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن (٢٠٠,٠٠٠) مائتي ألف درهم ولا تزيد على (٥٠٠,٠٠٠) خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين)، وذلك بناء على نتائج جريمة الاختراق نفسها، حيث نلاحظ أن المشرع الإماراتي قد شدد العقوبة في الفقرة الثالثة في حال كانت نتيجة جريمة الاختراق بغرض الحصول على المعلومات والبيانات واستخدامها لغرض غير مشروع، وهنا يمكن القول بأن المشرع الإماراتي يعتد بالباعث في جريمة الاختراق فالباعث يكون تعبير عن الحالة النفسية لمرتكب الجريمة وعليه ترى الباحثة أن الباعث في جريمة الاختراق هو الحصول على البيانات والمعلومات بغرض الحصول على بيانات لاستخدامها بغرض غير مشروع.

وفي حكم للمحكمة الاتحادية العليا:" محكمة الموضوع "ما تلتزم به". عقوبة "عقوبة تكميلية". غرامة. مصادرة. حكم "تسبيب سائغ". قانون "ما لا يقبل من الأسباب". العقوبة التكميلية. عقوبة تضاف إلى العقوبة الأصلية بهدف الحصول على مزيد من الردع والإصلاح ولا يقضي بها إلا بعد الحكم بإدانة المتهم ومعاقبته بإحدى العقوبات الأصلية المنصوص عليها قانوناً. أساس ذلك - تعذر ضبط الأشياء والأموال محل المصادرة. تحكم المحكمة بالغرامة المساوية لقيمتها - لا تحكم بمصادرة الأشياء والأموال المضبوطة إذا كانت مملوكة للمجني عليه وتسلم إليه في المطالبة المدنية بالتعويض أو رد مثلها. قضاء الحكم المطعون فيه بإدانة المطعون ضدهن ومعاقبتهم بالحبس دون مصادرة الأموال وعدم الحكم بغرامة مساوية لقيمة المال المسروق المملوك للمجني عليه أصاب صحيح القانون"[٣٦].

كما تنص المادة (٣) من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ على أنه:"

١) يعاقب بالسجن المؤقت والغرامة التي لا تقل عن (٢٠٠,٠٠٠) مائتي ألف درهم ولا تزيد على (٥٠٠,٠٠٠) خمسمائة ألف درهم، كل من اخترق موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات عائدة لمؤسسات الدولة.
٢) وتكون العقوبة السجن مدة لا تقل عن (٥) خمس سنوات والغرامة التي لا تقل عن (٢٥٠,٠٠٠) مائتين وخمسين ألف درهم ولا تزيد على (١,٥٠٠,٠٠٠) مليون وخمسمائة

[٣٦] (١) دولة الإمارات العربية المتحدة - المحكمة الاتحادية العليا - الأحكام الجزائية[الطعن رقم ٤٣٦ - لسنة ٢٠١٩ - تاريخ الجلسة ٢٠١٩/١١/١٨] [رفض]

ألف درهم، إذا ترتب على الاختراق إحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات أو خسارة سريتها أو وقعت الجريمة نتيجة لهجمة إلكترونية.

٣) وتكون العقوبة السجن المؤقت مدة لا تقل عن (٧) سنوات والغرامة التي لا تقل عن (٢٥٠,٠٠٠) مائتين وخمسين ألف درهم ولا تزيد على (١,٥٠٠,٠٠٠) مليون وخمسمائة ألف درهم، إذا كان الاختراق بغرض الحصول على البيانات أو المعلومات الخاصة بتلك الجهات المنصوص عليها بالفقرة الأولى من هذه المادة."

٣) وتكون العقوبة السجن المؤقت مدة لا تقل عن (٧) سنوات والغرامة التي لا تقل عن (٢٥٠,٠٠٠) مائتين وخمسين ألف درهم ولا تزيد على (١,٥٠٠,٠٠٠) مليون وخمسمائة ألف درهم، إذا كان الاختراق بغرض الحصول على البيانات أو المعلومات الخاصة بتلك الجهات المنصوص عليها بالفقرة الأولى من هذه المادة."

كما أنه من خلال ما ورد في الفقرة الثانية من المادة (٣) ترى الباحثة أن المشرع الإماراتي تبيع أسلوب التدرج في تشديد العقوبة على جريمة اختراق المواقع الإلكترونية حيث أنه انتقل من عقوبة السجن المؤقت غير محدد المدة إلى عقوبة السجن المؤقت لمدة (٥) سنوات والغرامة التي لا تقل عن (٢٥٠,٠٠٠) مائتين وخمسين ألف درهم ولا تزيد على (١,٥٠٠,٠٠٠) مليون وخمسمائة ألف درهم، وهنا نلاحظ أن المشرع الإماراتي قد شدد من الغرامة ويعود السبب في ذلك إلى رغبة المشرع الإماراتي في الحد من جريمة اختراق المواقع الإلكترونية الحكومية، إذا ترتب على الاختراق إحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات أو خسارة سريتها أو وقعت الجريمة نتيجة لهجمة إلكترونية.

ومن خلال ما ورد في الفقرة الأولى من هذه المادة يتضح أن المشرع الإماراتي يميز بين الاختراق لمواقع المؤسسات الحكومية وهي غرض العقوبة في المادة (٣) وبين جريمة اختراق المواقع غير الحكومية وهي مناط التجريم في المادة (٢)، وعليه من خلال ما ورد في الفقرة الأولى من المادة (٣) نجد أن المشرع الإماراتي قد نص على بعض العقوبات الأصلية على جريمة اختراق مواقع المؤسسات الحكومية، وهي بالطبع من العقوبات التي تختلف عما ورد في المادة (٢)، حيث يعاقب المشرع الإماراتي بعقوبة السجن والغرامة التي لا تقل عن (٢٠٠ ألف درهم)، ولا تزيد على نصف مليون درهم، وهنا نلاحظ أن المشرع الإماراتي في نص الفقرة الأولى من المادة (٣) على منح القاضي سلطة تقديرية بين الحبس أو الغرامة أو كلاهما، وبرأي الباحثة يرجع السبب في ذلك إلى أن المشرع الإماراتي يدرك خطورة جريمة اختراق المواقع الحكومية، كما يلاحظ أن المشرع الإماراتي في نص الفقرة الأولى من المادة (٣) قد بين نوع جريمة الاختراق التي تستوجب هذه العقوبة، وهي (كل من اخترق موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات عائدة لمؤسسات الدولة.)

وقد جاء في قضاء المحكمة الاتحادية العليا:" ... لمحكمة الموضوع السلطة التامة في تحصيل فهم الواقع في الدعوى واستخلاص ثبوت الجريمة من عدمه ... ولها مطلق الحرية في تكوين عقيدتها

من الأدلة والقرائن المطروحة في الدعوى، ولما كان البين من الحكم المطعون فيه أنه قد أحاط بواقع الدعوى عن بصر وبصيرة وبين عناصر الجريمة القانونية والواقعية اللتين أدين بهما الطاعن وأورد على ثبوتهما في حقه الأدلة القانونية الكافية والتي لها مأخذها الصحيح من أوراق الدعوى ومن شأنها أن تؤدى إلى ما رتبه الحكم عليها ... وقد أبدى الحكم اطمئنانه إلى ثبوت الجريمة في حقه وتوافر أركانها بما للمحكمة من سلطة وحرية في تكوين عقيدتها وبطريق الاستنتاج أو الاستقراء وكافة الممكنات العقلية وقد تبنت مستندات الحكم المستأنف الذي استعرض أقوال المتهم الطاعن لدى النيابة العامة من أنه يتحدث مع المتهم الثاني على انه فتاة مما يعد ذلك من المعاصي التي من شأنها أن تفسد الدين والأخلاق والذي أوجب لها المشرع التعزير بموجب ما نص عليه بالمادة ٣/٣١٢ من قانون العقوبات الاتحادي بما يكون وعلى النحو السالف بأن الجريمة اكتملت أركانها وقام الدليل الصحيح اليقيني على ثبوتها في حقه واستناداً لكل ذلك أدانته محكمة أول درجة بالاتهام المسند إليه وأيدته في ذلك محكمة الحكم المطعون فيه وحيث إن ما خلص إليه الحكم المطعون فيه بنى على أسباب سائغة وله أصله الثابت بالأوراق بما يكفي لحمله وفيه الرد الضمني المسقط لما أثاره الطاعن في دفاعه وكان الطعن مجرد جدل موضوعي لا يجوز إثارته أمام المحكمة العليا [٣٧].

ومن خلال ما ورد في الفقر الثالثة من المادة (٣) نلاحظ أن المشرع الإماراتي نص على عقوبة عن تائج اختراق مواقع المؤسسات الحكومية حيث أن العقوبة المقررة لذلك هي السجن المؤقت لمدة لا تقل عن (٧) سنوات والغرامة التي لا تقل عن (٢٥٠,٠٠٠) مائتين وخمسين ألف درهم ولا تزيد على (١,٥٠٠,٠٠٠) مليون وخمسمائة ألف درهم، وهنا تلاحظ الباحثة أيضاً أن المشرع الإماراتي كما فعل في الفقرة الأولى من المادة (٣) لم ينص على السلطة التقديرية للقاضي في عقوبة السجن المؤقت والغرامة وجعل الحكم بهما معاً إلزامياً، والسبب في ذلك برأي الباحثة إلى أن المشرع الإماراتي يدرك خطورة جريمة اختراق المواقع الإلكترونية الحكومية. كما أن المشرع الإماراتي قدد على سبيل الحصر ما يكن أن يترتب على جريمة اختراق المواقع الإلكترونية الحكومية وهو :" إذا كان الاختراق بغرض الحصول على البيانات أو المعلومات الخاصة بتلك الجهات المنصوص عليها بالفقرة الأولى من هذه المادة."."

وقد قضت المحكمة الاتحادية العليا في أحكامها بحرية القاضي الجزائي في تكوين اقتناعه مؤكدة أنه يتمتع بسلطة واسعة في جمع الأدلة وتقديرها في مجال الجرائم التعزيرية، فلا يتبع ترتيباً معيناً في الأخذ بها[١]، ويستطيع أن يستند إلى دليل دون الأدلة الأخرى، ففهم الواقع في الدعوى وتقدير أدبتها وترجيح ما تراه المحكمة راجحاً وجديراً بالاعتبار واستخلاص الحقيقة منها يدخل في اختصاص محكمة الموضوع دون رقابة عليها[٣٨]

---

[٣٧] جلسة الأحد الموافق ٢٤ من أكتوبر سنة ٢٠١٠ الطعن رقم ١٦٠ لسنة ٢٠١٠ جزائي.

[١] المحكمة الاتحادية العليا، نقض جزائي، جلسة ١٩٨٤/٦/٢٥، الطعن رقم ١٩ لسنة ٦ ق.ع، جزائي، جلسة ١٩٩٤/٣/٢٣.

[٣٨] المحكمة الاتحادية العليا، نقض جزائي، جلسة ١٩٩٣/٣/٦، الطعن رقم ١٦٢ لسنة ١٩٩١م، ق.ع. شرعي.

بينما في القانون المصري رقم (١٧٥) لسنة ٢٠١٨ فقد عرف الاختراق بأنه:" الاختراق: الدخول غير المرخص به أو المخالف لأحكام الترخيص، أو الدخول بأي طريقة غير مشروعة إلى نظام معلوماتي أو حاسب آلي أو شبكة معلوماتية وما في حكمها."

ومن هذه المادة نبين العقوبات التي جاء بها المشرع المصري لجريمة الاختراق عن طريق الدخول غير المصرح به والدخول بطريقة غير شرعية على النحو الآتي:

تنص المادة (١٤) من القانون المصري على أنه: يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدا، أو دخل بخطأ غير عمدي وبقى بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه. فإذا نتج عن ذلك الدخول إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي، تكون العقوبة الحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين."

ومن هذه المادة يتضح أن المشرع المصري يعاقب على جريمة الدخول غير المشروع للأنظمة المعلوماتية بعقوبة الحبس الذي لا تقل فيه المدة عن سنة والغرامة التي لا يقل حدها الأدنى عن (٥٠ ألف جنيه) ولا يتجاوز (١٠٠ ألف جنيه) وهذه العقوبة هي للدخول غير العمدي.

وقد جاء في قضاء المحكمة الاتحادية العليا حول السلطة التقديرية للقاضي الجنائي فيما يتعلق بالدليل الإلكتروني: "لما كان من المقرر في قضاء هذه المحكمة أن القاضي في المواد الجزائية يملك سلطة واسعة وحرية كاملة في سبيل فهم الواقع في الدعوى وتقدير أدلة الاتهام والوقوف على علاقة المتهم ومدى صلته بالجريمة وله مطلق الحرية لتكوين عقيدته عن الصورة من الأدلة قولية أو فنية أو قرائن بل له أن يركن في تكوين عقيدته إلى الصورة المحيطة لواقعة الدعوى واستظهار الحقائق القانونية المتعلقة بها من جماع العناصر المطروحة بطريق الاستنتاج والاستقراء وكافة الممكنات العقلية ما دام استخلاصه سليما لا يخرج عن الاقتضاء العقلي والمنطق؛ لما كان ذلك وكان الحكم المطعون فيه قد بين واقعة الدعوى بما تتوافر به كافة العناصر القانونية للجريمة التي دان بها الطاعنتين وأورد على ثبوتها في حقهما أدلة سائغة لها معينها الصحيح من أوراق الدعوى ومن شأنها أن تؤدي إلى ما رتبه الحكم عليها واستند في إدانة الطاعنتين بما هو منسوب إليهما على أقوال المجني عليها بالتحقيقات وأمام محكمة أول درجة من أن الطاعنتين قامتا بسبها بألفاظ السباب المبينة في الأوراق وذلك عن طريق برنامج التواصل الاجتماعي " الاحتساب " والرسائل النصية عبر هاتفيهما، وقد تأيدت هذه الأقوال بما جاء في تقرير المختبر الجنائي والذي أثبت قيام الطاعنتين بسب وقذف المجني عليها. وكان ما خلص إليه الحكم المطعون فيه قد جاء بأسباب سائغة مما له أصله الثابت بالأوراق بما يكفي لحمل قضائه ومن ثم فإن النعي في جملته ينحل إلى جدل موضوعي فيما لمحكمة الموضوع من سلطة فهم الواقع وتقدير الأدلة في الدعوى وهو ما لا يجوز إثارته أمام هذه المحكمة ويكون النعي قائما على غير أساس متعينا رفضه"[٣٩].

[٣٩] الطعنان رقما ٢٨٥ ، ٢٨٨ لسنة ٢٠١٨ جزائي- جلسة / / ٢٠١٨ م.

أما عقوبة الدخول المتعمد فقد حددها المشرع المصري بالحبس مدى لا تقل عن سنتين وغرامة حدها الأدنى مائة ألف جنيه وحدها الأعلى (٢٠٠) ألف جنيه.

وفي حال تجاوز مدة الدخول المصرح بها فقد نصت المادة (١٥) من القانون المصري على أنه:" يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتي مستخدما حقا مخولا له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول."

ومن هذه المادة يتضح أنَّ المشرع المصري نص على عقوبة الحبس التي لا تقل عن ستة أشهر والغرامة التي لا تتجاوز ثلاثون ألف جنيه مصري.

المطلب الثاني

العقوبات التبعية والتكميلية لجريمة اختراق المواقع الإلكترونية الحكومية

العقوبات التبعية: "هي عبارة عن جزاء ثانوي يلحق بالمحكوم عليه بقوة القانون، ودون حاجة لأن ينطق بها القاضي، وتستهدف تدعيم العقوبة الأصلية، ومن ثم لا يتصور توقيعها بمفردها[٤٠]. ولقد نظم المشرع الإماراتي الأحكام الخاصة بالعقوبات التبعية في المواد (٧٤ - ٨٠) من قانون الجرائم والعقوبات الاتحادي، وقد نصت المادة (٧٤) من ذات القانون على أن: "العقوبات التبعية هي:

١. الحرمان من بعض الحقوق والمزايا.
٢. العزل من الوظيفة العامة.
٣. مراقبة الشرطة."

بينما **يقصد بالعقوبة التكميلية**: "تلك العقوبة التي تكمل العقوبة الأصلية، ولا يتصور توقيها بمفردها، وإنما يتوقف تطبيقها على نطق القاضي بها. أي لا يجوز تنفيذها على المحكوم عليه إذا لم ينص عليها في الحكم، ولذلك لم يجعل المشرع أمر هذه العقوبات متحققة بقوة القانون، وإنما اشترط للحكم بها أن ينطق بها القاضي صراحة في الحكم الذي يصدره". ولقد نص المشرع الإماراتي على أنواع العقوبات التكميلية في المواد (٨١ و٨٢ و٨٣) من قانون الجرائم والعقوبات.

والفرق بين العقوبات التبعية والعقوبة التكميلية هو ان العقوبة التبعية هي التي تتبع بقوة القانون عقوبة أصلية محكوم بها على الجاني، فلا يشترط أن ينص عليها في الحكم، بل هي تقع بقوة القانون كأثر للحكم بالعقوبة الأصلية. ومن أمثلتها الحرمان من بعض الحقوق والمزايا ومراقبة الشرطة والعزل من الوظيفة العامة كأثر للحكم بعقوبة الجناية. بينما العقوبات التكملية هي عقوبات لا تلحق المحكوم عليه إلا إذا كان هناك عقوبة أصلية محكوم بها عليه، ولكنها تختلف عن العقوبة التبعية في أنها لا تتقرر بقوة القانون؛ وإنما يجب أن ينص القاضي عليا في الحكم مع العقوبة الأصلية. ومن أمثلتها المصادرة والعزل من الوظائف العمومية

---

(٤٠) – الدكتور/ محمود نجيب حسني، شرح قانون العقوبات القسم العام، دار النهضة العربية، القاهرة، ١٩٩٢، ، ص ٧٩٢.

حدد المشرع الإماراتي في نص المادة (٥٩) عقوبة حرمان الجاني من استخدام شبكة الإنترنت أو المواقع الإلكترونية لمدة محددة حيث تنص هذه المادة على أنه:" يجوز للمحكمة عند الحكم بالإدانة في أي جريمة من الجرائم المنصوص عليها بهذا المرسوم بقانون أن تقضي بأي من التدابير الآتية:

١) الأمر بوضع المحكوم عليه تحت الإشراف أو المراقبة الإلكترونية ***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.***

٢) إغلاق الموقع المخالف إغلاقا كليا أو جزئيا متى أمكن ذلك فنيا.

٣) حجب الموقع المخالف حجبا كليا أو جزئيا للمدة التي تقررها المحكمة.

يعاقب بالحبس مدة لا تزيد على سنة أو بغرامة لا تزيد على (٥٠٠٠) خمسة آلاف درهم، كل من خالف أي تدبير من التدابير المحكوم بها، وللمحكمة أن تأمر بإطالة التدبير مدة لا تزيد على نصف المدة المحكوم بها ولا تزيد في أية حال على (٣) ثلاث سنوات أو أن تستبدل به تدبيرا آخر مما ذكر."

من خلال الفقرة الأولى تلاحظ الباحثة أن المشرع الإماراتي نص على عقبة تبعية تختص المحكمة بإصدارها وهي عقوبة الحرمان من استخدام الشبكة أو الأنظمة المعلوماتية لفترة معينة تحدد الحكمة مدتها، والحرمان من هذا الاستخدام يكون بهدف إشعار الجاني بخطورة الجريمة التي ارتكبها، وحتى لا يعود على ارتكابها مرة أخرى.

ومن خلال الاطلاع على القانون المصري نجد أنه لا يتضمن اية عقوبات من هذا النوع وخاصة أنه يخلو من عقوبة المراقبة الإشراف.

ولكنه نص على عقوبة حجب المواقع حيث تنص المادة (٧) من القانون المصري على أنه:" لجهة التحقيق المختصة متى قامت أدلة على قيام موقع يبث داخل الدولة أو خارجها، بوضع أي عبارات أو أرقام أو صور أو أفلام أو أي مواد دعائية أو ما في حكمها، بما يعد جريمة من الجرائم المنصوص عليها في هذا القانون، ويشكل تهديدا للأمن القومي أو يعرض أمن البلاد أو اقتصادها القومي للخطر، أن تأمر بحجب الموقع أو المواقع محل البث، كلما أمكن تحقيق ذلك فنيا.

وعلى جهة التحقيق عرض أمر الحجب على المحكمة المختصة، منعقدة في غرفة المشورة خلال أربع وعشرين ساعة مشفوعا بمذكرة برأيها. وتصدر المحكمة قرارها في الأمر مسببا إما بالقبول أو بالرفض، في مدة لا تجاوز اثنتين وسبعين ساعة من وقت عرضه عليها.

ويجوز في حالة الاستعجال لوجود خطر حال، أو ضرر وشيك الوقوع، أن تقوم جهات التحري والضبط المختصة بإبلاغ الجهاز، ليقوم بإخطار مقدم الخدمة على الفور بالحجب المؤقت للموقع أو المحتوى أو المواقع أو الروابط المذكورة في الفقرة الأولى من هذه المادة وفقا لأحكامها. ويلتزم مقدم الخدمة بتنفيذ مضمون الإخطار فور وروده إليه.

وعلى جهة التحري والضبط التي قامت بالإبلاغ أن تحرر محضرا تثبت فيه ما تم من إجراءات وفق أحكام الفقرة السابقة يعرض على جهات التحقيق خلال ثمان وأربعين ساعة من تاريخ الإبلاغ الذي وجهته للجهاز، وتتبع في هذا المحضر ذات الإجراءات المبينة بالفقرة الثانية من هذه المادة، وتصدر المحكمة المختصة قرارها في هذه الحالة إما بتأييد ما تم من إجراءات حجب، أو بوقفها.

فإذا لم يعرض المحضر المشار إليه في الفقرة السابقة في الموعد المحدد، يعد الحجب الذي تم كأن لم يكن. ولمحكمة الموضوع أثناء نظر الدعوى، أو بناء على طلب جهة التحقيق أو الجهاز أو ذوي الشأن أن تأمر بإنهاء القرار الصادر بالحجب، أو تعديل نطاقه. وفي جميع الأحوال، يسقط القرار الصادر بالحجب بصدور أمر بألا وجه لإقامة الدعوى الجنائية، أو بصدور حكم نهائي فيها بالبراءة."

ومنه فإن كلاً من المشرع الإماراتي والمشرع المصري نصا على حجب المواقع كعقوبة تكميلية لجريمة الاختراق.

وقد أيّدت المحكمة الاتحادية العليا صفة عقوبة المصادرة بأنّها من العقوبات التكميلية في حكم لها جاء فيه:" لما كان ذلك وكانت المادة ٨٢ من قانون العقوبات قد جاءت تحت العقوبات التكميلية التي تضاف إلى العقوبة الأصلية بهدف الحصول على مزيد من الردع والإصلاح، ولا يقضى بها إلا بعد الحكم بإدانة المتّهم ومعاقبته بإحدى العقوبات الأصلية المنصوص عليها قانوناً، كما أنّ هذا النوع من العقوبات تفرض على الجرائم التي يتصوّر فيها تنفيذ هذا النوع من العقوبات. وحيث إنّ المادة المشار إليها قد نصّت في بدايتها على أنّ الحكم يكون بمصادرة الأشياء والأموال المضبوطة التي استعملت في الجريمة أو كان من شأنها أن تستعمل أو كانت محلاّ لها أو التي تحصّلت منها فإذا تعذّر ضبط أي من تلك الأشياء أو الأموال حكمت المحكمة بغرامة تعادل قيمتها بما مفاده أنّ الغرامة التي عناها المشرّع يصار إليها عند تعذّر ضبط الأشياء والأموال محل المصادرة وهو مالا يتصوّر في الجرائم التي يكون المال المضبوط مملوكاً للمجني عليه، فأوجب المشرّع إعادته لصاحبه، ولا تتم مصادرته، فالمصادرة هي نزع لملكية المال الذي اكتسب بطريقة مشروعة بالتصرف فيه أو إتلافه أو إدخاله في خزينة الدولة، فأوجب المشرّع في حالة تعذّر ضبطها تغريم الجاني بما يعادل قيمتها، أمّا الأشياء المملوكة للمجني عليه فلا محل لتغريم الجاني في حالة تقدير ضبطها وإنّما ينشئ حقاً للمجني عليه في المطالبة المدنية بالتعويض أو رد مثلها، ومن ثم فلا يقضى بالغرامة المساوية لقيمة المال المسروق في مثل هذه الجرائم. وحيث إنّه بالنظر إلى الواقعة محل الجريمة، فالثابت أنّها جريمة اختلاس وقضى الحكم المطعون فيه بإدانة المطعون ضده بالحبس فيها دون الأمر بمصادرة الأموال ولم يحكم بغرامة مساوية لقيمة المال المسروق، فإنّه يكون قد أصاب صحيح القانون"[٤١].

يشترط في الشيء الذي يقضي بمصادرته أن يكون مضبوطًا من قبل ضماناً لأن يصادف الحكم بالمصادرة محلاً وتحقيقاً من قابليته للتنفيذ وتمكيناً للقضاء من معاينته للتحقّق من توافر شروط المصادرة فيه، وبالتالي لا تجوز مصادرة الأشياء التي لم تضبط بعد كما لا يجوز الزام المحكوم عليه بدفع قيمتها، ويكفي بأن يكون الشيء قد ضبط ولو لم يكن تحت بصر المحكمة وقت الحكم.

كما بينت الفقرة الأولى من نص المادة (٦٦) من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن الشائعات والجرائم الإلكترونية إجراءات الحرمان من استخدام المواقع والشبكات ونظم المعلومات حيث نصت على أنه:" ١. في الأحوال التي تنقضي فيها الدعوى الجزائية بالتصالح أو الصلح وفقا لأحكام هذا المرسوم بقانون، للنائب العام ***أن يأمر بوضع المتهم تحت الإشراف أو***

---

[٤١] المحكمة الاتحادية العليا - الأحكام الجزائية - الطعن رقم ٦٨٤ لسنة ٢٠١٩ قضائية بتاريخ ٢٠١٩-١١-٠٩ [رفض]

المراقبة أو حرمانه من استخدام أي شبكة معلوماتية، أو نظام المعلومات الإلكتروني، أو أي وسيلة تقنية معلومات أخرى، أو إخضاعه لأحد برامج التأهيل للمدة التي يراها مناسبة."

كما أن المشرع الإماراتي في نص المادة (٥٦) من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ يعاقب بنوع آخر من أنواع العقوبات التكميلية وهي عقوبة المصادرة، حيث تنص هذه المادة على أنه:" مع عدم الإخلال بحقوق الغير حسنى النية، وفي حال الإدانة يحكم بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا المرسوم بقانون أو الأموال المتحصلة منها، وبحذف المعلومات أو البيانات."

ومن هذه المادة ترى الباحثة أن المشرع الإماراتي يعاقب بمصادرة الأجهزة التي تمت خلالها جريمة الاختراق، كما أن للمحكمة أن تأمر بحذف كل ما هو مرتبط بالجريمة.

كما ان المشرع المصري نص على عقوبة المصادر في المادة (٣٨) من القانون رقم (١٧٥) لسنة ٢٠١٨ حيث تنص على أنه:" مع عدم الإخلال بحقوق الغير حسن النية، على المحكمة في حالة الحكم بالإدانة في أي جريمة من الجرائم المنصوص عليها في هذا القانون أن تقضي بمصادرة الأدوات والآلات والمعدات والأجهزة مما لا يجوز حيازتها قانونا، أو غيرها مما يكون قد استخدم في ارتكاب الجريمة، أو سهل أو ساهم في ارتكابها. وفي الحالات التي يتعين لمزاولة النشاط فيها الحصول على ترخيص من إحدى الجهات الحكومية، وكان الشخص الاعتباري المدان بأي جريمة منصوص عليها في هذا القانون لم يحصل على الترخيص فيحكم فضلا عن العقوبات المقررة بالغلق."

في حكم للمحكمة الاتحادية العليا في إمارة أبوظبي جاء فيه: "لما كان نص المادة ٨٢ من قانون العقوبات الاتحادي يجري على أنّ للمحكمة عند الحكم بالإدانة في جناية أو جنحة أن يحكم بمصادرة الأشياء المضبوطة التي تحصّلت من الجريمة أو التي استعملت فيها أو التي كان من شأنها أن تستعمل فيها وذلك كله دون الإخلال بحقوق الآخرين.."[٤٢]."

المطلب الثالث

ظروف التشديد والتخفيف والإعفاء من العقوبة لجريمة اختراق المواقع الإلكترونية الحكومية

الأعذار المخففة: هي حالات حدد الشارع على سبيل الحصر يلتزم فيها القاضي بأن يهبط بالعقوبة المقررة للجريمة وفقا لقواعد معينة في القانون. ويقتصر أثره هذه الأعذار على من توافرت فيه من المساهمين في الجريمة وهي تنقسم إلى أعذار عامة تسري في حق كل الجرائم، وأخرى خاصة تقتصر على جريمة أو طائفة معينة من الجرائم ومن أمثلة الأعذار العامة عذر صغر من المتهم؛ إذ يؤدى توافره إلى النزول بالعقوبة إلى حدود أدنى من تلك المقررة للجريمة بينما الظروف المخففة: الظروف المخففة عبارة عن حالات تخفف من جسامة الجريمة، وتكشف عن خطورة

---

[٤٢] الطعن رقم ١٨٧ لسنة ٢٠١٥ س ٩ ق. أ، جلسة ٢٢-٣-٢٠٢٥ جزائي، المحكمة الاتحادية العليا، المكتب الفني، أبوظبي، ص ١٥١.

فاعلها، وتستوجب أو تجيز للقاضي تخفيف العقوبة أو الحكم بتدبير يناسب تلك الخطورة وأساس هذه الظروف، هو تمكين القاضي من تحقيق الملاءمة بين العقوبة وجسامة الجريمة

إن الغاية من نص المشرع الإماراتي على ظروف التشديد في عقوبة الاختراق هو الحد من هذا النوع من الجرائم الإلكترونية، وتحقيق الردع العام والخاص بما يسهم في حماية مواقع مؤسسات الدولة من أي جريمة قد تؤثر على خدمات تلك المواقع.

أسباب تخفيف العقاب هي حالات يجب فيها على القاضي أو يجوز له أن يحكم من أجل الجريمة بعقوبة أخف في نوعها أو أدنى في مقدارها عن تلك المقررة لها أصلاً وتنقسم أسباب تخفيف العقوبة إلى نوعين: أسباب تخفيف وجوبية يطلق عليها الأعذار القانونية وقد نص عليها القانون على سبيل الحصر، وأسباب تخفيف جوازيه يطلق عليها بالظروف القضائية المخففة، والفرق الجوهري بينهما أن التخفيف عند توافر العذر القانوني إلزامي للقاضي، في حين أنه جوازي عند توافر الظروف القضائية يترك أمر تقديرها لقاضي الموضوع.

الأعذار المخففة هي حالات محددة في القانون على سبيل الحصر ويلتزم القاضي عند توافرها بأن يهبط بالعقوبة المقررة للجريمة وفقاً لقواعد معينة في القانون[٤٣].

وهي عبارة عن ظروف وملابسات تتعلق بشخص الجاني أو بحالته النفسية، أو تلك التي ترجع إلى الجريمة المسندة إليه، ويرى المشرع أن توافرها وقت ارتكاب الجريمة، يستوجب تخفيف العقوبة عليه، ولذلك نص عليها على سبيل الحصر، وعينها تعييناً لا يترك معه للقاضي أي سلطة تقديرية بشأن استخلاصها من ظروف الدعوى ووقائعها[٤٤].

وقد قضت المحكمة الاتحادية العليا في أحكامها بحرية القاضي الجزائي في تكوين اقتناعه مؤكدة أنه يتمتع بسلطة واسعة في جمع الأدلة وتقديرها في مجال الجرائم التعزيرية، فلا يتبع ترتيباً معيناً في الأخذ بها[٤٥]، ويستطيع أن يستند إلى دليل دون الأدلى الأخرى، ففهم الواقع في الدعوى وتقدير أدبتها وترجيح ما تراه المحكمة راجحاً وجديراً بالاعتبار واستخلاص الحقيقة منها يدخل في اختصاص محكمة الموضوع دون رقابة عليها[٤٦].
تعرف الظروف المخففة بأنها أسباب يستخلصها القاضي من وقائع الدعوى الجزائية التي يحكم فيها أو من ظروف المتهم شخصياً لتخفيف العقوبة عن الحد الأدنى المقرر للجريمة[٤٧]، وذلك في الحدود التي قررها القانون في المادتين (٩٩ و١٠١) من قانون الجرائم والعقوبات. ولم يحدد المشرع الإماراتي هذه الأسباب ولم يضع ضوابط تعين القاضي على استخلاصها، وإنما ترك أمر تقديرها للمحكمة تستخلصها من ظروف وملابسات كل جريمة بشكل مستقل. ومن الأمثلة على الظروف المخففة التقديرية ارتكاب الجريمة لأول مرة، ندم الجاني على فعله، صلح الجاني مع الجني عليه، ظروف الجاني الأسرية، كبر من الجاني .... الخ.

---

[٤٣] – الدكتور/ محمود نجيب حسني، مرجع سابق، ص ٩١٧.
[٤٤] – الدكتور/ مصطفى الجوهري، مرجع سابق، ص ٢٨١.
[٤٥] المحكمة الاتحادية العليا، نقض جزائي، جلسة ١٩٨٤/٦/٢٥، الطعن رقم ١٩ لسنة ٦ ق.ع، جزائي، جلسة ١٩٩٤/٣/٢٣.
[٤٦] المحكمة الاتحادية العليا، نقض جزائي، جلسة ١٩٩٣/٣/٦، الطعن رقم ١٦٢ لسنة ١٩٩١م، ق.ع. شرعي.
[٤٧] – الدكتور/ محمود نجيب حسني، مرجع سابق، ص ٩١٩.

وترجع عدالة تقرير الظروف المخففة في منح القاضي سلطة تقديرية للملائمة بين نصوص الأمازون المجردة، وبين الظروف الواقعية التي أحاطت ارتكاب الجريمة عند تقدير العقوبة التي يجب فرضها على الجاني، وهي بهذا الخصوص تنسجم مع أهداف العقوبة التي من بينها تحقيق العدالة، التي لا تتحقق إلا من خلال فرض عقوبة تتناسب مع الجريمة المرتكبة ومع ظروف الجاني الشخصية.

وتطبيقاً لذلك، قضت المحكمة الاتحادية العليا بأنه: "من المقرر في قضاء هذه المحكمة أن تقدير العقوبة وتقدير موجبات الرأفة أو عدم قيامها من اختصاص محكمة الموضوع دون معقب عليه ودون أن تسأل عن الأسباب التي من أجلها أوقعت العقوبة بالقدر الذي ارتأته ولا رقابة عليها في ذلك متى التزمت حدود العقوبة المنصوص عليها قانونا"[٤٨].

وقد بين المشرع الإماراتي حالة واحدة للتخفيف من العقوبة في جريمة الاختراق نصت عليها المادة (٦١) من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ حيث تنص على أنه:" ١. تقضي المحكمة، بناء على طلب من النائب العام، ***بتخفيف العقوبة أو بالإعفاء منها، عمن أدلى من الجناة إلى السلطات القضائية أو الإدارية بمعلومات تتعلق بأي جريمة من الجرائم المنصوص عليها في هذا المرسوم بقانون، متى أدى ذلك إلى الكشف عن الجريمة ومرتكبيها أو إثباتها عليهم أو القبض على أحدهم.***

٢. وفي الجرائم الماسة بأمن الدولة للنائب العام للاتحاد دون غيره أن يطلب من المحكمة المنظورة أمامها الدعوى إعمال حكم الفقرة السابقة في غير الحالات المنصوص عليها فيها، إذا تعلق الطلب بالمصلحة العليا للدولة أو بأي مصلحة وطنية أخرى، فإذا صدر حكم في الدعوى جاز له أن يقدم الطلب إلى المحكمة التي أصدرته قبل التنفيذ أو أثناء التنفيذ."

ومن خلال الفقرة الأولى من هذه المادة يتضح أن المشرع الإماراتي أجاز للمحكمة تخفيف العقوبة في حالة عمن أدلى من الجناة إلى السلطات القضائية أو الإدارية بمعلومات تتعلق بأي جريمة من الجرائم المنصوص عليها في هذا المرسوم بقانون، متى أدى ذلك إلى الكشف عن الجريمة ومرتكبيها أو إثباتها عليهم أو القبض على أحدهم" وهنا ترى الباحثة أن هذه الحالة وحدها غير كافية وكان الأجدر أن يحدد المشرع الإماراتي حالات خاصة بالإبلاغ يمكن الاستناد إليها من قبل المحكمة في تخفيفها للعقوبة.

تعرف الظروف المشددة للعقاب بأنها حالات يجب فيها على القاضي - أو يجوز له - أن يحكم بعقوبة من نوع أشد مما يقرره القانون للجريمة، أو يجاوز الحد الأقصى الذي نص عليه القانون كعقوبة لهذه الجريمة[٤٩].

وترجع علة تشديد العقوبة إلى تمكين القاضي من تحقيق ملائمة كاملة بين العقوبة التي ينطق بها والظروف الواقعية للدعوى، التي تتطلب مزيداً من التشديد يجاوز ما يسمح به القانون في النص الخاص بالجريمة، بهدف تحقيق التناسب بين العقوبة التي يستحقها الجاني ودرجة جسامة الفعل وخطورة الجاني[٥٠].

---

[٤٨] – الاتحادية العليا جلسة ٢٠٠٥/٦/٢، القضية رقم ١٠٦ لسنة ٢٦ القضائية، شرعي جزائي.

[٤٩] – الدكتور/ محمود نجيب حسني، مرجع سابق، ص ٩٢٨.

[٥٠] – للمزيد حول ذلك بالتفصيل راجع: الدكتورة/ ماجدة فؤاد محمود، الظروف المشددة، دراسة تحليلية مقارنة، رسالة دكتوراه، سنة ١٩٨٨، جامعة عين شمس، مصر، ص ٣٩٢ وما بعدها.

تنقسم الظروف المشددة للعقاب إلى قسمين: ظروف مشددة خاصة ينحصر نطاقها في جريمة أو جرائم معينة، وظرف مشددة عامة ينصرف أثرها لكافة الجرائم أو أغلبها. سنبين هذين النوعين على النحو الآتي:

١. الظروف المشددة الخاصة:

وهي التي بينها المشرع في صدر نص المادة (١٠٣) من قانون الجرائم والعقوبات الاتحادي في قوله: "مع مراعاة الأحوال التي يبين فيها القانون أسباب خاصة للتشديد..". ويتميز هذا النوع من الظروف بأن نطاق تطبيقه يقتصر على جريمة أو جرائم معينة، وهي عديدة ومتنوعة بعدد الجرائم التي يقرر المشروع بالنسبة لها توافر هذه الظروف، ومثال ذلك الظروف تلك التي ترجع إلى جسامة الجانب المادي للجريمة، كان يستخدم الجاني السم في ارتكاب جريمة القتل العمد، وقد ترجع هذه الخطورة إلى ارتكاب السلوك الإجرامي في مكان معين، كالسرقة من مكان مسكون أو من دور العبادة، أو ارتكابه في زمن معين كالسرقة ليلاً وحمل السلاح وظرف تعدد الجناة التي تشدد عقوبة جريمة السرقة.

ويعتبر من قبيل هذه الظروف المشددة الخاصة كذلك ظرف سبق الإصرار أو الترصد أو كون المجني عليه أحد أصول الجاني ترتب على ذلك تشديد العقاب إلى الإعدام بدلاً من السجن المؤبد أو المؤقت. ومثلها كذلك ما يعود إلى إخلال الجاني بصفة معينة تطلبها المشرع فيه، كصفة الخادم في السرقة، وصفة الطبيب أو الجراح أو الصيدلي أو القابلة في الإجهاض. ويعتبر القسم الخاص من قانون العقوبات الموضع المناسب لدراسة الظروف المشددة الخاصة، إذ تلحق بكل جريمة على حدة أركانها وعقوبتها والظروف المشددة لها أو الأعذار المخففة أو المعفية منها.

٢. **الظروف المشددة العامة**: هي تلك الظروف أو الأسباب التي يقررها المشرع، ويكون من شأن توافرها تشديد العقاب، وينصرف أثرها إلى جميع الجرائم أو أغالبها. وقد نظم المشرع الإماراتي أحكام هذه الظروف في المواد (١٠٣ - ١٠٥) من قانون الجرائم والعقوبات الاتحادي.

تنص المادة (١٠٣) من القانون ذاته على أربعة أنواع من الظروف المشددة العامة بقولها: "مع مراعاة الأحوال التي يبين فيها القانون أسباباً خاصة للتشديد يعتبر من الظروف المشددة ما يلي:

أ- ارتكاب الجريمة بباعث دنيء.

ب- ارتكاب الجريمة بانتهاز فرصة ضعف إدراك المجنى عليه، أو عجزه عن المقاومة أو في ظروف لا تمكن غيره من الدفاع عنه.

ج- ارتكاب الجريمة باستعمال طرق وحشية أو التمثيل بالمجني عليه.

د- وقوع الجريمة من موظف عام استغلالاً لسلطة وظيفته أو لصفته ما لم يقرر القانون عقاباً خاصاً اعتباراً لهذه الصفة.

ويتضح من هذا النص أن المشرع جعل من الخطورة الإجرامية الخاصة في شخص الجاني، أو اتصافه بالخسة أو الوحشية في ارتكابه للجريمة، أو إساءته لسلطات وظيفته إن كان موظفة عامة واستغلالها في ارتكاب الجريمة أساسا لتشديد العقاب[٥١].

---

[٥١] – الدكتور/ علي حمودة، مرجع سابق، ص ١٣٦.

وقد بين المشرع الإماراتي في المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ الظروف المشددة على جريمة الاختراق حيث تنص هذه المادة على أنه:" في تطبيق أحكام هذا المرسوم بقانون يعد ظرفا مشددا:

١) ارتكاب الجاني لأي جريمة منصوص عليها في هذا المرسوم بقانون بمناسبة أو بسبب تأدية عمله.
٢) استخدام الجاني شبكة المعلومات أو أي نظام معلوماتي إلكتروني أو موقع إلكتروني أو وسيلة تقنية معلومات عند ارتكاب أي جريمة لم ينص عليها هذا المرسوم بقانون.
٣) ارتكاب الجاني أي جريمة منصوص عليها في هذا المرسوم بقانون لحساب أو لمصلحة دولة أجنبية أو أي جماعة معادية أو جماعة إرهابية أو تنظيم غير مشروع."

ومن خلال ما ورد في نص هذه المادة ترى الباحثة أن ظروف التشديد على جريمة الاختراق تأتي لثلاثة مبررات قانونية نص عليها المشرع الإماراتي على سبيل الحصر، هي إذا ارتكبت جريمة الاختراق بمناسبة استغلال الوظف لوظيفته، والوسيلة التي ترتكب بها جريمة لم ينص عليها القانون أي أن يقوم الجاني باستخدام شبكة المعلومات ونظم المعلومات في ارتكاب جريمة إلكترونية لم ينص عليها القانون، وارتكاب الجريمة بغرض مساعدة التنظيمات الإرهابية، وهنا ترى الباحثة أن هناك الكثير من الأسباب الخاصة بتشديد عقوبة جرية اختراق المواقع الحكومية لم ينص عليها المشرع الإماراتي، على سبيل المثال أن يكون الاختراق بغرض الاعتراض أو تعطيل الشبكات أو يكون الاختراق بغرض سياسي أو أمني.

وبالرجوع لموقف المشرع المصري من ظروف التشديد نجد أنه جعلها في عدة حالات، الحالة الأولى نصت عليها الفقرة الأخيرة من المادة (٢١) من القانون المصري في جريمة الاعتداء على سلامة الشبكة المعلوماتية التي تنص على أنه:" فإذا وقعت الجريمة على شبكة معلوماتية تخص الدولة أو أحد الأشخاص الاعتبارية العامة أو تمتلكها أو تدار بمعرفتها تكون العقوبة السجن المشدد، وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه."

وهنا نلاحظ أن كلاً من المشرع الإماراتي والمشرع المصري يعتبران أن وقوع الجريمة على مواقع حكومية إحدى ظروف التشديد.

الحالة الثانية نصت عليها المادة (٣٠) من القانون المصري في نطاق المسئولية الجنائية لمقدمي الخدمة حيث تنص على أنه: يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه، أو بإحدى هاتين العقوبتين، كل مقدم خدمة امتنع عن تنفيذ القرار الصادر من المحكمة الجنائية المختصة بحجب أحد المواقع أو الروابط أو المحتوى المُشار إليه في الفقرة الأولى من المادة (٧) من هذا القانون. فإذا ترتب على الامتناع عن تنفيذ القرار الصادر من المحكمة، وفاة شخص أو أكثر، أو الإضرار بالأمن القومي، تكون العقوبة السجن المشدد، والغرامة التي لا تقل عن ثلاثة ملايين جنيه ولا تجاوز عشرين مليون جنيه، وتقضي المحكمة فضلا عن ذلك بإلغاء ترخيص مزاولة النشاط."

الحالة الثالثة نصت عليها المادة (٣٤) من القانون المصري التي تنص على أنه:" إذا وقعت أي جريمة من الجرائم المنصوص عليها في هذا القانون بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر أو الإضرار بالأمن القومي للبلاد أو بمركزها الاقتصادي أو منع أو

عرقلة ممارسة السلطات العامة لأعمالها أو تعطيل أحكام الدستور أو القوانين أو اللوائح أو الإضرار بالوحدة الوطنية والسلام الاجتماعي، تكون العقوبة السجن المشدد."

وعليه يمكن القول بان المشرع المصري لم يتوسع بحالات وظروف تشديد العقوبة على جريمة الاختراق كما فعل المشرع الإماراتي.

كما ان المشرع الإماراتي نص على ظروف مشدد للعقوبة في المادة (٥) من القانون التي تنص على أنه:" يعاقب بالسجن المؤقت والغرامة التي لا تقل عن (٥٠٠,٠٠٠) خمسمائة ألف درهم ولا تزيد على (٣,٠٠٠,٠٠٠) ثلاثة ملايين درهم، كل من تسبب عمدا في الإضرار أو تدمير أو إيقاف أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، عائدة لمؤسسات الدولة أو أحد المرافق الحيوية. ***فإذا وقعت الجريمة نتيجة لهجمة إلكترونية أعتبر ذلك ظرفا مشددا."***

ومن نص هذه المادة ترى الباحثة أن المشرع الإماراتي قد نص على ظرف مشدد للعقوبة ولكنه لم يدرجه في نص المادة (٣٤) التي بينت ظروف التشديد، وأن اعتبار المشرع الإماراتي الهجمات الإلكترنية سبباً للتشديد في جرائم الاختراق له ما يبرره وخاصة أن جرائم الاختراق لا تتم عادة إلا من خلال هجمات إلكترونية تستهدف المواقع الحكومية. وكذلك فعل المشرع المصري في القانون رقم (١٧٥) لسنة ٢٠١٨ بشأن جرائن تقنية المعلومات حيث تنص الفقرة الأخيرة من المادة (٢١) منه على أنه:" فإذا وقعت الجريمة على شبكة معلوماتية تخص الدولة أو أحد الأشخاص الاعتبارية العامة أو تمتلكها أو تدار بمعرفتها تكون العقوبة السجن المشدد، وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه." ومنه يمكن القول بأن كلاً من المشرع الإماراتي والمشرع المصري أخذا بذات الاتجاه فيما يتعلق بظروف التشديد.

كما أن المشرع الإماراتي أيضاً نص على ظرف آخر من ظروف التشديد في المادة (٦) من القانون التي تنص على أنه:" ١. يعاقب بالحبس مدة لا تقل عن (٦) ستة أشهر والغرامة التي لا تقل عن (٢٠,٠٠٠) عشرين ألف درهم ولا تزيد على (١٠٠,٠٠٠) مائة ألف درهم، أو بإحدى هاتين العقوبتين، كل من حصل أو استحوذ أو عدل أو أتلف أو أفشى أو سرب أو ألغى أو حذف أو نسخ أو نشر أو أعاد نشر بغير تصريح بيانات أو معلومات شخصية إلكترونية، باستخدام تقنية المعلومات أو وسيلة تقنية معلومات. ***فإذا كانت البيانات أو المعلومات المشار إليها في البند (١) من هذه المادة، تتعلق بفحوصات أو تشخيص أو علاج أو رعاية أو سجلات طبية أو حسابات مصرفية أو بيانات ومعلومات وسائل الدفع الإلكترونية عد ذلك ظرفا مشددا."*** كما أن المشرع المصري لم ينص على مثل هذه الحالة الخاصة بالتشديد في القانون رقم (١٧٥) لسنة ٢٠١٨ وهنا يمكن القول بأن المشرع الإماراتي قد تفرد بهذا الظرف الخاص بالتشديد ولم يأخذ به المشرع المصري.

وهنا ترى الباحثة أيضاً أن المشرع الإماراتي قد نص على ظرف من ظروف التشديد، ولكنه لم يدرجه في سياق المادة (٣٤) التي نصت على ظروف التشديد للعقوبة، كما أن موضوع التشديد الوارد في المادة (٦) له ما يبرره وخاصة أن الاعتداء على المعلومات المالية قد يتم عن طريق الاختراق، وهنا ترى الباحثة أنه كان الأجدر أن يقوم المشرع الإماراتي بإضافة جريمة اختراق المؤسسات المالية وإدراجها ضمن المادة (٣) من القانون كونها تتعلق بمؤسسات الدولة.

عرف المشرع المصري في المادة الأولى من القانون رقم (١٧٥) لسنة ٢٠١٨ بشأن جرائم تقنية المعلومات الاختراق بأنه:" الاختراق: الدخول غير المرخص به أو المخالف لأحكام الترخيص، أو الدخول بأي طريقة غير مشروعة إلى نظام معلوماتي أو حاسب آلي أو شبكة معلوماتية وما في حكمها."

الخاتمة

تناول البحث موضوع البنيان القانوني لجريمة اختراق المواقع الإلكترونية الحكومية بالتحليل على ضوء أحكام المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن الشائعات والجرائم الإلكترونية بالمقارنة مع أحكام القانون المصري رقم (١٧٥) لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، وفي نهاية البحث توصلنا لبعض النتائج والتوصيات على النحو الآتي:

أولاً: النتائج:

١) المشرع الإماراتي قد بين ماهية الاختراق بأنه فقعل الدخول غير المشروع بشكل غير مرخص أو الدخول بترخيص لكن بشكل مخالف لأحكام الترخيص على أن يكون هذا الدخول للمواقع الإلكترونية الحكومية يتصف بعدم المشروعية، وحدد المشرع الإماراتي خلال التعريف محل الدخول غير المشروع بأن يكون إلى نظام الحاسب الآلي أو نظام التشغيل للآلات والأجهزة أو شبكة المعلومات أو أية شيء يكون بحكمها، وهنا يمكن القول بأن المشرع الاماراتي يعتبر الاختراق هو الفعل المجرم وأن الدخول غير المشروع إلى الأنظمة المعلوماتية هو الغاية أو الوسيلة لارتكاب جريمة الاختراق، وقد أحسن المشرع الإماراتي في تعريفه للاختراق على هذا النحو.

٢) جريمة الاختراق الإلكتروني هي مقدمة لجرائم أخرى، حيث أنه من غير المتصور أن ترتكب جريمة الاختراق دون أن يكون الهدف منها هو اتجاه إرادة مرتكب الجريمة إلى تحقيق نتيجة معينة من جراء الاختراق.

٣) المشرع الإماراتي أخذ بمبدأ تشديد العقوبة على جريمة اختراق الأنظمة المعلوماتية للمؤسسات الحكومية في حال نتج عنها أي من النتائج السابقة، وهنا يمكن القول بأن الأحكام الخاصة بجريمة اختراق الأنظمة المعلوماتية للمؤسسات الحكومية تميل إلى التشديد وفق النتيجة الإجرامية التي تنتج عن فعل الاختراق ذاته.

٤) المشرع الإماراتي تبيع أسلوب التدرج في تشديد العقوبة على جريمة اختراق المواقع الإلكترونية حيث أنه انتقل من عقوبة السجن المؤقت غير محدد المدة إلى عقوبة السجن المؤقت لمدة (٥) سنوات والغرامة التي لا تقل عن (٢٥٠,٠٠٠) مائتين وخمسين ألف

درهم ولا تزيد على (١,٥٠٠,٠٠٠) مليون وخمسمائة ألف درهم، وهنا نلاحظ أن المشرع الإماراتي قد شدد من الغرامة ويعود السبب في ذلك إلى رغبة المشرع الإماراتي في الحد من جريمة اختراق المواقع الإلكترونية الحكومية، إذا ترتب على الاختراق إحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات أو خسارة سريتها أو وقعت الجريمة نتيجة لهجمة إلكترونية.

ثانياً: التوصيات.

١) قيام المشرع الإماراتي بتعريف الاختراق في نص المادة الأولى من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠١١.

٢) تتمنى الباحثة على المشرع الإماراتي أن يضيف مادة في المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن الشائعات والجرائم الإلكترونية تبين ماهية الاختراق ودوافعه لأن ما ورد في القانون فيما يخص الاختراق يبين أن الاختراق ليس جريمة مستقلة بل هو فعل سابق لجريمة القرصنة أو الإتلاف المعلوماتي ما يتسبب بالخلط بين تلك الأفعال. وتقترح الباحثة أن يكون تعريف الاختراق:" الهجوم الإلكتروني الواقع على منظومة معلوماتية بهدف الدخول غير المرخص به أو المخالف لأحكام الترخيص أو الدخول بطريقة غير مشروعة أو البقاء بصورة غير مشروعة في نظام معلوماتي أو حاسب آلي أو نظام تشغيل جهاز أو آلة أو مركبة أو شبكة معلوماتية وما في حكمها"

٣) تتمنى الباحثة على المشرع الإماراتي أن يضع جريمة الاختراق المعلوماتي وحدها كجريمة مستقلة عن باقي الجرائم، كون ما ورد في القانون يخلط بين الاختراق والبقاء غير المشروع، كما تقترح الباحثة نصاً لهذه المادة على النحو الآتي:" الاختراق هو الهجوم الذي يتم خلاله الدخول للمنظومة المعلوماتية ويتسبب بالنتائج التالية: "الإتلاف" و"التدمير" و"التخريب" و "محو البرامج والبيانات" و"التشويه" و"مسح البرامج والبيانات" و"إيقاف" أو "حذف" أو أي سلوك آخر يجعل البيانات أو المعلومات أو البرامج والمحررات المعلوماتية غير صالحة للاستعمال كلياً أو جزئياً. "

٤) تتمنى الباحثة على المشرع الإماراتي أن يفرق بين جريمة الاختراق وجريمة الدخول غير المشروع حيث أن الدخول غير المشروع له فعل واحد هو الولوج للمنظومة المعلوماتية،

بينما الاختراق قد يكون عن طريق عدة أفعال منها الهاكرز والهجوم السيبراني حتى وإن كان محل الجريمة واحداً في الاختراق والدخول غير المشروع.

قائمة المراجع

أولاً: الكتب العامة

١) طارق العبدالله: شرح قانون الجرائم والعقوبات الاتحادي، دار النهضة العلمية، القاهرة، ٢٠٢٢، ص ١١٢
٢) عبد العزيز أحمد الحسن، شرح قانون الجرائم والعقوبات الاتحادي لدولة الإمارات العربية المتحدة الصادر بموجب المرسوم بقانون اتحادي رقم ٣١ لسنة ٢٠٢١، الأحكام العامة، الكتاب الأول، النظرية العامة للجريمة، دار النهضة العلمية ٢٠٢٢، ص (١٤١
٣) عبد الغني قاسم مثنى الشعيبي، شرح قانون الجرائم والعقوبات لدولة الإمارات العربية المتحدة الصادر بمرسوم بقانون اتحادي رقم (٣١) لسنة ٢٠٢١، القسم العام، النظرية العامة للجريمة والنظرية العامة للجزاء الجنائي، مكتبة دار الحافظ، الإمارات العربية المتحدة، ٢٠٢٢ م،
٤) علي حمودة، شرح قانون العقوبات، أكاديمية شرطة دبي، دبي، ٢٠١٥.
٥) محمد الجبور: الوسيط في قانون العقوبات، القسم العام، الطبعة الأولى، دار وائل، عمان، ٢٠١٢م،
٦) محمد الجندين مقال "خصائص البيانات الضخمة"، مجلة لغة العصر، جريدة الأهرام، العدد ٢٣٩، القاهرة، أكتوبر ٢٠١٦م.
٧) محمود نجيب حسني – النظرية العامة للقصد الجنائي، دار النهضة العربية، القاهرة، ١٩٩٢.
٨) محمود نجيب حسني، شرح قانون العقوبات القسم العام، دار النهضة العربية، القاهرة، ١٩٩٢،
٩) مصطفى الجوهري، شرح قانون العقوبات العام، دار النهضة العربية، القاهرة، ٢٠١٢

ثانياً: الكتب المتخصصة

١) إبراهيم محمود اللبيدي: السلوك الإجرامي في جرائم الإنترنت، مركز الإعلام الأمني، القاهرة،
٢) أمير فرج يوسف، جرائم تقنية المعلومات بدول الخليج العربي والجهود الدولية والمحلية لمكافحة جرائم الإنترنت والحاسوب الإلكترونية في دول الخليج العربي، دار الكتب والدراسات العربية، الطبعة الأولى ٢٠١٥م، ص٢١٨
٣) جميل الصغير : جرائم الإنترنت، دار النهضة العربية، القاهرة، ٢٠١٤،
٤) خالد حربي السعدي: جريمة إتلاف برامج ومعلومات الحاسب الآلي في التشريعين الكويتي والمقارن ، دار النهضة العربية، القاهرة، ٢٠١٢،
٥) خالد سامي السيد : الأمن القومي الإلكتروني وجرائم المعلومات ـــ دار النهضة العربية – القاهرة – مصر – الطبعة الأولى – ٢٠٢١
٦) دكتور خالد سامي السيد : الأمن القومي الإلكتروني وجرائم المعلومات ـــ دار النهضة العربية – القاهرة – مصر – الطبعة الأولى – ٢٠٢١
٧) راشد محمد المري : الجرائم الإلكترونية، دار النهضة العلمية ودار النهضة العربية ، مصر والإمارات ، ط١ ، ٢٠١٨م

٨) شمسان ناجي صالح الخيلي : الجرائم المستخدمة بطرق غير مشروعة لشبكة الإنترنت ـــ دار النهضة العربية – القاهرة – مصر – ٢٠١٩
٩) عبد الفتاح بيومي حجازي: الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، المركز القومي للإصدارات القانونية، مصر، ٢٠١١م،
١٠) عبير شفيق الرحباني: الجرائم الإلكترونية ومخاطرها، دار الثقافة للنشر والتوزيع، عمان، ط١، ٢٠٢٠م،
١١) عمار عباس الحسيني : جريمة الإتلاف المعلوماتي ـــ مكتبة زين الحقوقية الأدبية – بيروت – لبنان – الطبعة الأولى – ٢٠١٩م
١٢) محمد خليفة: الحماية الجنائية لمعطيات الحاسب الآلي، دار النهضة العربية، القاهرة، ٢٠١٩،
١٣) محمود رجب فتح الله: الوسيط في الجرائم المعلوماتية دار الجامعة الجديدة الطبعة الأولى، سنة ٢٠١٨،

الرسائل العلمية

١) أحمد قاسم، جريمة الدخول إلى منظومة معلوماتية، رسالة ماجستير، جامعة دمشق، ٢٠١٤-٢٠١٥ م
٢) عبد العزيز الحسن: علم النفس في علم الجريمة والجريمة، رسالة دكتوراه ، جامعة روبرت شومان في ستراسبورغ، ١٩٩٨.
٣) ماجدة فؤاد محمود، الظروف المشددة، دراسة تحليلية مقارنة، رسالة دكتوراه، سنة ١٩٨٨، جامعة عين شمس، مصر،
٤) محمد عبد الله محمد العوا: المسئولية الجنائية الناشئة عن جرائم الأموال عبر الانترنت، رسالة دكتوراه بكلية الحقوق جامعة الاسكندرية، ٢٠١٢،

البحوث والمقالات

١) عبيد صالح حسن، سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية، الفكر الشرطي، القيادة العامة لشرطة الشارقة، المجلد ٢٤، العدد رقم ٩٥، اكتوبر ٢٠٢٢ م،

القوانين

١) دولة الإمارات العربية المتحدة - مرسوم بقانون اتحادي - رقم ٣٤ لسنة ٢٠٢١ الصادر بتاريخ ٢٠٢١-٠٩-٢٠ نشر بتاريخ ٢٠٢١-٠٩-٢٦ يعمل به إعتبارا من ٢٠٢٢-٠١-٠٢ بشأن مكافحة الشائعات والجرائم الإلكترونية. الجريدة الرسمية ٧١٢ ملحق - السنة الواحد والخمسون
٢) القانون المصري رقم (١٧٥) لسنة ٢٠١٨ بشأن جرائم تقنية المعلومات
٣) المرسوم بقانون اتحادي رقم (٣٠) لسنة ٢٠٢١ بشأن الجرائم والعقوبات

الأحكام القضائية

١) الاتحادية العليا جلسة ٢٠٠٥/٦/٢، القضية رقم ١٠٦ لسنة ٢٦ القضائية، شرعي جزائي.
٢) جلسة الأحد الموافق ٢٤ من أكتوبر سنة ٢٠١٠ الطعن رقم ١٦٠ لسنة ٢٠١٠ جزائي.
٣) دولة الإمارات العربية المتحدة - المحكمة الاتحادية العليا - الأحكام الجزائية[الطعن رقم ٤٣٦ - لسنة ٢٠١٩ - تاريخ الجلسة ٢٠١٩/١١/١٨] [رفض]

٤) الطعن رقم ١٨٧ لسنة ٢٠١٥ س ٩ ق. أ، جلسة ٢٢-٣-٢٠٢٥ جزائي، المحكمة الاتحادية العليا، المكتب الفني، أبوظبي، ص ١٥١.
٥) الطعنان رقما ٢٨٥ ، ٢٨٨ لسنة ٢٠١٨ جزائي- جلسة / / ٢٠١٨ م.
٦) المحكمة الإتحادية العليا - الأحكام الجزائية - الطعن رقم ١٢٨٥ لسنة ٢٠٢٠ قضائية بتاريخ ٢٠٢١-٠٣-٠١ [رفض الطعن]
٧) المحكمة الإتحادية العليا - الأحكام الجزائية - الطعن رقم ١٨٥ لسنة ٢٠١١ قضائية بتاريخ ٢٠١١-٠٦-٢١ [رفض]
٨) المحكمة الإتحادية العليا - الأحكام الجزائية - الطعن رقم ١٨٥ لسنة ٢٠١١ قضائية بتاريخ ٢٠١١-٠٦-٢١ [رفض]
٩) المحكمة الاتحادية العليا - الأحكام الجزائية - الطعن رقم ٦٨٤ لسنة ٢٠١٩ قضائية بتاريخ ٢٠١٩-١١-٠٩ [رفض]
١٠) المحكمة الاتحادية العليا، نقض جزائي، جلسة ١٩٨٤/٦/٢٥، الطعن رقم ١٩ لسنة ٦ ق.ع، جزائي، جلسة ١٩٩٤/٣/٢٣.
١١) المحكمة الاتحادية العليا، نقض جزائي، جلسة ١٩٨٤/٦/٢٥، الطعن رقم ١٩ لسنة ٦ ق.ع، جزائي، جلسة ١٩٩٤/٣/٢٣.
١٢) المحكمة الاتحادية العليا، نقض جزائي، جلسة ١٩٩٣/٣/٦، الطعن رقم ١٦٢ لسنة ١٩٩١م، ق.ع. شرعي.
١٣) المحكمة الاتحادية العليا، نقض جزائي، جلسة ١٩٩٣/٣/٦، الطعن رقم ١٦٢ لسنة ١٩٩١م، ق.ع. شرعي.
١٤) محكمة التمييز - الأحكام الجزائية - الطعن رقم ١٢٨١ لسنة ٢٠١٩ قضائية - الدائرة الجزائية - بتاريخ ٢٠٢١-٠١-٢٤
١٥) محكمة التمييز - الأحكام الجزائية - الطعن رقم ٢٣٠ لسنة ٢٠٠١ قضائية - الدائرة الجزائية - بتاريخ ٢٠٠١-١٢-٠٨ مكتب فني ١٢ رقم الجزء ١ رقم الصفحة ١٢٦٦ [رفض] رقم القاعدة ٥٧
١٦) محكمة التمييز - الأحكام الجزائية - الطعن رقم ٥٤٠ لسنة ٢٠١٧ قضائية - الدائرة الجزائية - بتاريخ ٢٠١٧-٠٩-٢٥ مكتب فني ٢٨ رقم الصفحة ٤٦٣ [نقض الحكم والإحالة] رقم القاعدة ٥٨

المراجع الأجنبية

1) Martin Wasik, The Computer Misuse Act 1990-The Criminal Law review, Manchester Uni. 1990.
2) Guillaume Champy, La fraude informatique, tome 1, () Presses Universitaires d Aix-Marseille, 51992, p. 88.
3) PETER SWIFT: HACK MAN MENACE OF THE KEYBOARD CRIMINAL BRITICH TELECOM WORLD MAG, HALF OF SEPT 1989 P 13-14.
4) Buffelan - Lanore: La Procédure Apllicable Aux Infraction Commises Par Les Personnes Morales Rev, Sociétés 1993. P. 315 ets.