جمهوريّة مصر العربيّة
جامعة المنصورة
كليّة الحقوق
قسم القانون الجنائي

أركان جريمة اختراق المواقع الرسمية الإلكترونية في التشريع الإماراتي دراسة مقارنة

بحث ضمن متطلبات الحصول على درجة الدكتوراه في الحقوق

تحت إشراف

الأستاذ الدكتور

أحمد شوقي عمر أبو خطوة

أستاذ القانون الجنائي وعميد كلية الحقوق الأسبق

كلية الحقوق جامعة المنصورة

إعداد الباحث

عمر عبد الله محمد الطنيجي

1447هـ/٢٠٢٥م

المقدمة

شرع المشرّع في دولة الإمارات باتخاذ تدابير متكاملة لمجابهة الجرائم الإلكترونية، وكانت أولى هذه الخطوات إصدار المرسوم بقانون رقم (٢) لسنة ٢٠٠٦، الذي تناول بشكل محدد الجرائم المرتبطة بتقنية المعلومات [١]، ثم جرى تعديله لاحقًا من خلال المرسوم بقانون رقم (٥) لسنة ٢٠١٢ [٢]،إلى أن صدر في نهاية المطاف المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ الذي تناول مكافحة الشائعات والجرائم الإلكترونية[٣]، هكذا اعتاد المشرع في دولة الإمارات على مواجهة الجريمة بشكل عام، فهي ليست ظاهرة طارئة على حياة الإنسان، بل صاحبت وجوده منذ بدايته على الأرض، منذ حادثة قتل قابيل لهابيل. ومع مرور الزمن وتغير المجتمعات، تطورت الجرائم وظهرت أنواع وطرق جديدة لم تكن معروفة من قبل، مما جعل من الضروري على الجهات المختصة أن تقوم بتحديث القوانين والأنظمة والإجراءات بشكل مستمر لمواكبة هذا التطور والتصدي له[٤].

رغم التقدم الكبير في تقنيات نقل وتبادل المعلومات، وسعي كثير من الدول نحو تطبيق نظم الحكومة الرقمية، إلا أن الاستخدام الخاطئ لهذه التكنولوجيا أصبح يشكل خطراً على خصوصية الحكومات، من خلال العبث بمعلوماتها أو تخريبها أحياناً، وتسريبها ونشرها في أحيان أخرى، وذلك عبر الهجمات على مواقعها الإلكترونية الرسمية.

ودولة الإمارات، شأنها شأن غيرها من الدول، لم تكن بمنأى عن هذه الظاهرة، إذ تعرضت مواقعها الرسمية في الفترة الأخيرة لهجمات واختراقات متكررة، وهو الأمر الذي لم يقتصر عليها فقط، فقط، بل طال دولًا عربية أخرى مثل مصر وغيرها.

ولكي نتمكن من اعتبار أن هناك جريمة قد وقعت، فلا بد من توافر عناصرها الأساسية، وهما:

---

(١) منشور في العدد رقم (٤٤٢) من الجريدة الرسمية.

(٢) مرسوم بقانون ٥ لسنة ٢٠١٢م بشأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية العدد ٥٤٠ ملحق السنة الثانية والأربعون – بتاريخ ٢٦-٨-٢٠١٢م.

(٣) صدر بقصر الرئاسة في أبوظبي، بتاريخ ١٣/ صفر/ ١٤٤٣ه، الموافق ٢٠/ سبتمبر/ ٢٠٢١م.

(4)Ibrahim El-Shahat Lotfy,"The crime of electronic hacking in UAE legislation", International Journal of Advanced Research on Law and Governance, Volume 5, Issue 2, 2023, P.p 176 - 200.

وهما: العنصر المادي، والعنصر المعنوي. فإذا كانت الجريمة مقصودة، فلا بد أن تتوفر لدى الفاعل نية إجرامية واضحة، تقوم على العلم بالفعل والإرادة في ارتكابه. وبناء على ذلك، فإن من يتعمد اختراق المواقع الرسمية وهو مدرك لطبيعة ما يفعله، تتحقق في حقه المسؤولية الجنائية عن هذا الفعل.

من الضروري أن نعي أن عالم الإنترنت يشمل عدة أطراف، فهناك من يتولى إعداد المحتوى الذي يُنشر، سواء كانوا أشخاصاً أم جهات رسمية أو خاصة مثل الوزارات أو الجامعات أو مراكز البحوث، وهناك أيضاً من يوفر إمكانية الوصول إلى هذا المحتوى، وهم مقدمو خدمات الإنترنت، سواء سواء كانوا شركات أم أفراداً أو مؤسسات. ومن هنا يثور تساؤل مهم: إلى أي مدى يكون كل طرف مسؤولًا جنائيًا عن ما يُنشر على الإنترنت؟ وهل يُساوى بين من أنشأ المحتوى وبين من أتاح الوصول إليه من حيث المسؤولية؟[٥].

ولا شك أن تقنيات المعلومات باتت في الفترة الأخيرة عنصراً محورياً تعتمد عليه مختلف جوانب الحياة، مثل الاقتصاد، والمجتمع، والسياسة، والزراعة، والصناعة. ومع التوسع المتزايد في استخدام الإنترنت، سواء عبر البيانات أم الوسائل الحديثة، بدأت تظهر أنماط جديدة من الجرائم تُعرف بالجرائم المعلوماتية، وهي نتيجة طبيعية لمواكبة التطور التكنولوجي والعلمي المستمر.

وتقوم هذه النوعية من الجرائم عموماً على جانبين رئيسيين: أولهما يوجّه نحو المال، وثانيهما يستهدف الأفراد، مستفيدة في ذلك من القدرات الكبيرة التي يوفرها الحاسب الآلي في تنفيذ هذه الأفعال[٦].

---

(٥) د. مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٠م، ص٥٣.

(٦) د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، ط٢، دار النهضة العربية، القاهرة، ١٩٩٨م، ص٤٥.

ونظراً للارتفاع المستمر في الهجمات التي يشنها القراصنة الإلكترونيون على المواقع الرسمية التابعة للدولة، يرى الباحث أن من المهم جعل حدود المسؤولية الجنائية المتعلقة بهذا النوع من الاعتداءات واضحة ، وذلك من خلال دراسة وتحليل مواد القانون الإماراتي ومقارنتها بما ورد في القانون المصري. وبناءً على ذلك، سيتم فيما يلي تناول أهمية هذا البحث، والقضايا المحورية التي يناقشها، إلى جانب التحديات التي واجهت الباحث أثناء عملية الإعداد، والمنهج المتبع في إجراء الدراسة، وأخيراً سيتم عرض الخطة التفصيلية للبحث كما يلي:

أولًا- أهمية البحث:

إن الانتشار الواسع لاستخدام شبكة الإنترنت في الفترة الأخيرة، سواء في الدول العربية أم الإسلامية، أدى إلى ظهور آثار متعددة، منها ما هو إيجابي ومنها ما هو سلبي، على مختلف المستويات، كالأمن، والمجتمع، والثقافة، والاقتصاد، والسياسة، إلى جانب بروز تحديات قانونية متزايدة، وتطور واضح في أساليب الجرائم الإلكترونية.

أوضح التحليل العام للشكاوى التي استقبلها مركز شكاوى احتيال الإنترنت في الولايات المتحدة أن المركز تلقى خلال أول ستة أشهر من انطلاقه ما مجموعه ٦٠٨٧ شكوى، وكان من بينها ٥٢٧٣ شكوى تتعلق باستخدام الحاسوب عبر الإنترنت (٧).

شهدت جرائم الاختراق الإلكتروني تزايداً ملحوظًا، سواء استهدفت موقعًا إلكترونيًا أم نظام معلومات أو شبكة إلكترونية أو أي وسيلة تقنية حديثة، بما في ذلك الأنظمة الخاصة بالمؤسسات الحكومية. ويُعد هذا التطور في الأساليب الإجرامية نتيجة مباشرة لاستخدام التكنولوجيا الحديثة، إذ يعمد المجرمون إلى الوصول إلى هذه الأنظمة والعبث بمحتواها، سواء عن طريق التغيير أم الإتلاف أو السرقة.

وقد دفع هذا الواقع العديد من الدول إلى إدخال تعديلات تشريعية تُجرّم مثل هذه الأفعال وتفرض عقوبات عليها، إدراكًا لما تحمله من تهديدات خطيرة. فكل دولة تمتلك معلومات حساسة لا

---

(٧) د. حسين بن سعيد الغافري: "السياسة الجنائية في مواجهة الإنترنت" دراسة مقارنة، دار النهضة، القاهرة، ٢٠٠٩م، ص٩.

يجب الاطلاع عليها دون تصريح أو مبرر قانوني، وأي اختراق لها قد يسبب أزمات على الصعيدين الداخلي والخارجي، نظراً لما تمثله من خطورة كبيرة(٨).

ثانيًا- مشكلة البحث:

مع التقدم المستمر في أنظمة الحاسب الآلي والانتشار الواسع لشبكة الإنترنت، وجد القراصنة والجماعات الإرهابية في هذا التطور فرصة لتوظيفه بشكل سلبي، حيث قاموا بتحويل الجرائم التقليدية إلى نمط أكثر تعقيداً من خلال ما يُعرف بالقرصنة الإلكترونية. ففي البداية، كانت هذه الأفعال تهدف إلى السرقة وتحقيق مكاسب غير مشروعة، لكنها سرعان ما تحولت إلى هجمات موجهة نحو المواقع الرسمية للدولة بهدف إحداث أضرار كبيرة، بل ومحاولة تدمير البنية التحتية للدول المستهدفة بكل صورها، فضلًا عن نشر الشائعات وإثارة الفوضى وزعزعة الاستقرار.

ومن هذا المنطلق تبرز أهمية هذا البحث، الذي يستند إلى فرضية أساسية مفادها أن اختراق المواقع الإلكترونية التابعة للحكومة يشكل تهديداً جديًا لكل ما تسعى الدولة إلى بنائه حاليًا، سواء من قواعد بيانات أم شبكات أو أنظمة رقمية حكومية. ويتسع هذا التهديد ليشمل منشآت حساسة مثل محطات الكهرباء، ومحطات تنقية المياه، ووسائل الاتصالات، ووسائل النقل، وشركات الطيران، والجهات الاقتصادية والمالية، والتي لا تزال تفتقر إلى الحماية الكافية في ظل التشريعات والأنظمة الحالية، مما يجعلها هدفًا سهلًا لهذه الهجمات.

من هنا تبرز ضرورة التعمق في فهم هذه الظاهرة وتحليل الأساليب التي تُرتكب بها، بهدف الوصول إلى حلول عملية واقتراح إجراءات فعالة تقلّل من آثارها السلبية. وتدور الإشكالية الأساسية لهذا البحث حول السؤال الجوهري التالي: ما هو الإطار القانوني الذي ينظّم الجريمة موضع الدراسة في كل من التشريعين الإماراتي والمصري؟

ثالثًا منهج البحث:

يعتمد هذا البحث على المنهج الوصفي التحليلي، الذي يقوم على رصد الواقع القائم وتحليل العوامل التي أدت إلى ظهور الجريمة موضع الدراسة، مع تقييم مدى قدرة النصوص القانونية الحالية على

---

(٨) د. سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م، ص٦٥.

مواجهتها بفعالية. إلى جانب ذلك، سيتم توظيف المنهج المقارن، من خلال إجراء مقارنة بين ما جاء به كل من القانون الإماراتي والمصري بشأن هذه الجريمة، بهدف إبراز أوجه الاتفاق والاختلاف في كيفية تعامل كل نظام قانوني معها.

رابعًا: خطة البحث:

وفي ضوء ما تقدم بيانه، فإننا نقسم خطة البحث على النحو التالي:

نظرًا لكون الجريمة **موضع الدراسة** تُعد من الجرائم التي لا تتحقق إلا بتوافر عنصرين أساسيين، وهما الركن المادي والركن المعنوي، فإن المسؤولية الجنائية عن ارتكابها لا تقوم إلا إذا اجتمع هذان العنصران معًا. وبناءً عليه، سيتناول هذا البحث تحليلًا مفصلًا لأركان هذه الجريمة وبيان مكوناتها.

المبحث الأول

الركن المادي لجريمة اختراق المواقع الإلكترونية

تمهيد وتقسيم:

يُعد الركن المادي جزءًا أساسيًا لا غنى عنه في تكوين أي جريمة، وبشكل خاص في الجريمة محل الدراسة، إذ لا يمكن تحميل الفاعل المسؤولية الجنائية ما لم يتحقق هذا العنصر. ولتحقيق ذلك، يجب أن يصدر عن الجاني فعل مادي واضح يُخالف القانون، وينتج عنه أثر محسوس، سواء كان هذا الأثر مباشرًا أم غير مباشر، ما دامت هناك علاقة سببية تربط بين التصرف والنتيجة. وفي بعض الحالات، لا يكون من الضروري وقوع نتيجة محددة، بل يكفي مجرد تنفيذ الفعل الممنوع لاعتبار الجريمة قائمة، كما هو الحال في الجرائم الشكلية، التي تُعد جريمة اختراق المواقع الرسمية نموذجًا لها[٩].

نص القانون الإماراتي في المادة (٣٢) من قانون العقوبات لسنة ٢٠٢١ على أن الركن المادي للجريمة يتحقق عندما يقوم الشخص بارتكاب فعل يخالف القانون، أو يمتنع عن القيام بعمل يفرضه

---

(٩) د. رفعت رشوان، سياسة المشرع الإماراتي الجنائية في مواجهة الجرائم البيئية، ندوة علمية حول مكافحة جرائم البيئة، القيادة العامة لشرطة أبو ظبي، مركز البحوث والدراسات الأمنية، ص ١٠١.

عليه القانون، بشرط أن يكون هذا السلوك، سواء أكان إيجابيًا أم سلبيًا، مُجرّمًا بنص صريح. ويعتمد هذا الركن على ثلاثة عناصر أساسية: الفعل الذي يصدر عن الجاني، والنتيجة التي تترتب على هذا الفعل، والعلاقة السببية التي تربط بينهما.

وتُعد الجريمة موضع الدراسة من الجرائم التي تندرج ضمن هذا الإطار، إذ تقوم على تصرف غير مشروع يصدر عن شخص، يؤدي إلى إحداث ضرر مباشر، وتكون هناك علاقة واضحة تربط بين الفعل والنتيجة. وقد بيّنت المحكمة العليا هذا المفهوم بقولها إن الجريمة عمومًا هي سلوك غير قانوني يتم عن وعي وإرادة، ويترتب عليه جزاء يقرره القانون. وعليه، فإن تحقق الركن المادي يتطلب أن يكون الفعل قد صدر فعليًا عن الجاني، وأن يكون مُجرّمًا، ومقرونًا بإرادة مدركة. أما إذا كان السلوك سلبيًا، كأن يتقاعس الشخص عن تنفيذ واجب قانوني، فيجب إثبات وجود صلة مباشرة بين هذا الامتناع والضرر الذي نتج عنه [١٠].

المطلب الأول

النشاط في جريمة اختراق المواقع الإلكترونية

السلوك الإجرامي هو التصرف الظاهر الذي يُعبّر عن النية الداخلية للجاني، ويُظهر ما كان مستترًا في نفسه، إذ إن القانون لا يُعاقب على مجرد الأفكار أو الرغبات أو النوايا ما دامت لم تخرج إلى الواقع في صورة فعل ملموس يمكن الاستدلال عليه. وينقسم هذا السلوك إلى شكلين: سلوك إيجابي يتمثل في القيام بفعل يترك أثرًا ماديًا في الواقع، وسلوك سلبي يتمثل في امتناع الشخص عن أداء واجب محدد كان ينبغي عليه القيام به وفقًا للقانون في ظرف معين، لكنه تعمّد تركه.

في جريمة اختراق المواقع الإلكترونية يتمثل التصرف الإجرامي في قيام الجاني بالدخول إلى الموقع دون الحصول على إذن أو تفويض، وهو ما يُعد سلوكًا غير قانوني. وغالبًا ما يتم هذا الدخول غير المصرح به من خلال تجاوز أو كسر كلمة المرور الخاصة بالموقع، وهي معلومة تكون حصرًا بيد الشخص المسؤول عن إدارة الموقع. وفي بعض الحالات، يلجأ الجاني إلى استخدام برامج خبيثة

---

(١٠) دولة الإمارات العربية المتحدة: المحكمة الاتحادية العليا، دائرة الأحكام الجزائية، الطعن رقم ٢٢٣، لسنة ٢٣ ق، بتاريخ ٢٠٠٣/٤/٢٦م.

تُثبت داخل نظام تشغيل الموقع وتعمل في الخلفية دون أن تُكتشف، بهدف التقاط وتسجيل بيانات الدخول التي يستخدمها المسؤول، وهو الشخص المخول بإدارة محتوى الموقع وآلية تشغيله وتنظيمه(١١).

ويقصد بالسلوك الإجرامي ذلك التصرف المادي الواضح الذي يصدر عن الجاني، سواء تمثل في قيامه بفعل معين، أم في امتناعه عن أداء واجب قانوني يُفترض به الالتزام به، مما يجعله معرضًا للمساءلة (١)، ويُفهم الفعل هنا – باعتباره جزءًا من الركن المادي – بمعناه الواسع، فقد يكون سلوكًا إيجابيًا يتمثل في حركة جسدية تصدر عن الجاني، كما قد يكون سلوكًا سلبيًا يظهر في صورة الامتناع عن أداء ما يفرضه عليه القانون. ويُعد هذا الفعل عنصرًا أساسيًا في الركن المادي للجريمة، سواء كانت الجريمة عمدية أم غير عمدية(١٢)، وبناءً على ما تقدم، يمكن تصنيف السلوك الإجرامي إلى شكلين رئيسيين: الأول هو السلوك الإيجابي، ويتمثل في قيام الجاني بفعل معين يشكل مخالفة، أما الثاني فهو السلوك السلبي، ويكون على صورة الامتناع عن القيام بفعل كان مطلوبًا منه قانونًا. وجريمة اختراق المواقع الإلكترونية تندرج ضمن هذا التصنيف، إذ يمكن ارتكابها بأي من الطريقتين. وقد جاء كل من القانون الإماراتي الصادر بموجب المرسوم الاتحادي رقم (٣٤) لسنة ٢٠٢١، والقانون المصري رقم (١٧٥) لسنة ٢٠١٨، بنصوص تُجرّم أفعالًا محددة تُعد اعتداءً على البيانات الرقمية، وهي تمثل في مضمونها تجسيدًا فعليًا للركن المادي في هذه الجريمة، سواء ارتُكبت بالفعل المباشر أم عن طريق امتناع يخالف أحكام القانون.

ويُعتبر الركن المادي في هذه الجريمة قائمًا بمجرد المساس بسرية المعلومات أو انتهاك خصوصيتها، حتى وإن لم يترتب على هذا الفعل نتيجة محددة؛ فهي جريمة تُعاقب على السلوك ذاته دون الحاجة لتحقق أثر أو ضرر لاحق، لأن الهدف الأساسي من هذا التجريم هو حماية الخصوصية

---

(١١) دلال لطيف مطشر، جريمة الاعتداء على المواقع الإلكترونية – دراسة مقارنة، مجلة جامعة بابل للعلوم الإنسانية، المجلد ٢٦، العدد ٩، ٢٠١٨م، ص٣٩٩ وما بعدها.

(١) د. أحمد عوض بلال، مبادئ قانون العقوبات المصري "القسم العام"، دار النهضة، القاهرة، بدون سنة نشر، ص٢٥٥.

(١٢) د. محمود نجيب حسني، شرح قانون العقوبات – القسم العام، دار النهضة العربية، القاهرة، ٢٠١٦م، ص٣٠٤.

والحفاظ على سرية البيانات. ومن هنا، تتضح أهمية مستوى الأمان الرقمي، فكلما كان تأمين البيانات أفضل، ارتفعت معه مستويات الاستقرار والأمن المجتمعي(١٣).

يتجسد العنصر المادي في جريمة اختراق المواقع الإلكترونية من خلال صور متعددة، أبرزها استخدام وسائل وأدوات تكنولوجية بهدف إحداث فعل مادي داخل البيئة الإلكترونية، سواء لإلحاق ضرر أم للتدخل غير المشروع في نظام معلوماتي. ويُشترط في هذا السياق أن يكون السلوك مرتبطًا ببيئة إلكترونية محددة أو واقعًا ضمن نطاق معلوماتي معين. ومن المهم التنويه إلى أن هذا النوع من الجرائم لا يتطلب بالضرورة وقوع ضرر فعلي، لأنها تُعد من الجرائم الشكلية، التي يكفي لقيامها ارتكاب الفعل المحظور ذاته، دون الحاجة إلى تحقق نتيجة محددة.

يتحقق السلوك الإجرامي عندما يُقدم شخص، أو مجموعة، أو جهة منظمة على أفعال تهدف إلى الإضرار بالمواقع الرسمية أو إحداث خلل في أنظمتها. وقد بيّنت المحكمة الاتحادية العليا أن الفرد يُعد فاعلًا أصليًا للجريمة إذا توفرت لديه نية المشاركة، وقام عمدًا بأي تصرف ساهم في تنفيذ الجريمة الإلكترونية، سواء تولى تنفيذها بالكامل أم شارك بجزء منها، مما يؤدي إلى استكمال الجانب المادي للجريمة(١٤).

وبناءً عليه، فإن من يرتكب جريمة إلكترونية يتحمل كامل المسؤولية عن كل ما يترتب عليها من نتائج، حتى لو ساهمت عوامل أخرى – سواء بصورة مباشرة أم غير مباشرة – في وقوع الضرر، طالما أن تلك العوامل لم تكن كافية وحدها لقطع الصلة بين السلوك الإجرامي والنتيجة المترتبة (١٥).

وتتعدد صور السلوك الإجرامي المرتبط بالجريمة محل الدراسة، حيث بدأت هذه الأفعال تتجلى بوضوح في المجتمع بوصفها تصرفات يعاقب عليها القانون. وقد حدد المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ المعني بمكافحة الشائعات والجرائم الإلكترونية هذه الأشكال على النحو التالي:

---

(١٣) د. ياسر نوار، المواجهة التشريعية والأمنية لجرائم التجارة الإلكترونية، ط١، بدون دار نشر، ٢٠١٢م، ص٧١.

(١٤) دولة الإمارات العربية المتحدة: المحكمة الاتحادية العليا، دائرة الأحكام الجزائية، الطعن رقم ٢٣، لسنة١٧ق، بتاريخ ١٩٩٥/٦/٣م.

(١٥) حكومة دبي: محكمة التمييز، دائرة الأحكام الجزائية، الطعن رقم ٢٢٩، لسنة ٢٠٠٣ ق، بتاريخ ٢٠٠٣/١٠/١٨م.

أولًا- الدخول غير المصرح به إلى المواقع الإلكترونية الرسمية للدولة:

يُعتبر الدخول غير المصرح به من أوضح الأفعال التي تُجسّد الجانب المادي في الجريمة موضع الدراسة ، حيث يُقصد به الدخول إلى أنظمة أو أجهزة أو شبكات إلكترونية دون الحصول على إذن، أو بما يخالف التصاريح الممنوحة، أو باستخدام طرق غير قانونية، أو حتى الاستمرار داخل هذه الأنظمة بطريقة غير مشروعة. ويُعد هذا النوع من السلوك من أخطر الجرائم الرقمية، لما يحمله من خطر كبير على خصوصية وسلامة المعلومات الحكومية، وتأثيره المباشر على أمن الدولة الإلكتروني، مما يستوجب وجود وسائل حماية فعّالة تصون المصالح العامة، وتُتيح للجهات المعنية تشغيل أنظمتها بثقة وأمان دون تدخلات غير قانونية [١٦].

يمكن تنفيذ اختراق الحواسيب أو انتحال هوية مستخدميها بوسائل مادية أو إلكترونية، فالاختراق المادي يتمثل في تمكن الجاني من دخول أماكن محمية عبر بوابات إلكترونية أو آلية، وغالبًا ما يتم ذلك بأن يتظاهر الجاني بحمل أدوات تخص أجهزة الحاسوب – مثل الأشرطة الممغنطة – أو أن يستغل لحظة دخول شخص مصرح له ويعبر البوابة معه في الوقت نفسه. ومن هنا يتبين أن التواجد الفعلي داخل غرف التحكم أو صالات الحواسيب يُعد شرطًا أساسيًا لارتكاب هذه الجرائم، حيث يكون التصرف غير القانوني منصبًا على ما تحويه هذه الأنظمة من بيانات ومعلومات محفوظة[١٧].

ثانيًا- الدعاية لكيفية فك الشفرة للأجهزة الإلكترونية الخاصة بمؤسسات وهيئات الدولة:

أشارت المادة رقم (١) من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ إلى أن التشفير هو عملية يتم فيها تحويل البيانات أو الأنظمة أو الأدوات التقنية إلى صيغة غير مفهومة، ولا يمكن استعادتها إلى حالتها الأصلية إلا باستخدام كلمة مرور أو أداة مخصصة لفك التشفير. ويُعد استخدام التشفير أحد الأساليب التي يُلجأ إليها في ارتكاب الجريمة محل البحث ، حيث يُستخدم للسيطرة على المعلومات والبيانات، إما بتعطيلها أو التلاعب بها، مما يؤدي إلى إلحاق أضرار كبيرة بتلك المواقع.

وكمثال تطبيقي على استخدام التشفير كوجه من أوجه النشاط الإجرامي، فقد حدث في نهاية

---

(١٦) د. هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقًا عليها، ط٢، دار النهضة العربية، القاهرة، ٢٠١١م، ص٤٩ وما بعدها.

(١٧) محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والإنترنت، منشأة المعارف، الإسكندرية، ٢٠٠٦م، ص١٤٤.

عام ١٩٨٤ أن مجلة فرنسية كانت تنوي تزويد قرائها بتعليمات فنية تساعدهم على صنع جهاز لفك الشفرات باستخدام أجزاء متفرقة، مما كان سيمكنهم من مشاهدة برامج إحدى القنوات المشفرة دون دفع رسوم الاشتراك. وعلى إثر ذلك، لجأت الشركة المالكة للقناة إلى القضاء، واعتبر القاضي أن ما تفعله المجلة تحريض على التحايل، ويعد تصرفًا غير قانوني يسبب ضرراً تجاريًا وشيكًا، فقرر وقف توزيع العدد الذي يتضمن هذا المحتوى المخالف فوراً [١٨]،في ذلك الوقت، انتقل المخطط الذي كانت تنوي مجلة "راديو بلان" نشره إلى جريدة "لو كوتيديان دو باري"، والتي سارعت بدورها إلى نشره في عددها الصادر يومي ٢٤ و٢٥ نوفمبر ١٩٨٤، واضعة إياه في أولى الصفحات تحت عنوان لافت: "اللعبة الجديدة الممنوعة لعطلة نهاية الأسبوع: اصنع بنفسك جهازاً لفك شفرة قناة كانال بلس"[١٩].

من الممكن اعتبار فعل توصيل جهاز فك الشفرة غير المرخص بجهاز الاستقبال كأنه يشكل عنصر "الاختلاس" – وهو أحد الجوانب المكونة للفعل المادي في جريمة السرقة – إلا أن هذا التفسير غير دقيق؛ لأن هذا النوع من التوصيل لا يؤثر في سيطرة المالك الأصلية على محتوى البرامج التي يواصل بثها، كما أنه لا يمنع المشاهد المشترك من استقبال تلك البرامج بشكل طبيعي. فبحسب ما رأت المحكمة، فإن جهاز فك الشفرة ما هو إلا وسيلة لتحسين جودة الاستقبال، ولا يُعد استخدامه تعدياً على الحق في مشاهدة البرامج التي يملك المشاهد حق الوصول إليها أصلاً[٢٠].

ثالثًا– إتلاف البرامج وتخريب المواقع الرسمية للدولة:

نص القانون الاتحادي رقم (٣٤) لسنة ٢٠٢١ في مادته الأولى على أن الهجمات الإلكترونية تُعد أفعالًا متعمدة ومنظمة تستهدف الأنظمة الرقمية أو الشبكات أو البنية التحتية التقنية، ويكون من شأنها التأثير على كفاءتها أو تعطيل أدائها. وتشمل هذه الأفعال ما يُرتكب بدوافع فردية، أو بغرض التسلل أو الاعتراض أو الاختراق أو التسريب، أو بهدف تعريض المعلومات للخطر أو إيقاف العمليات

---

(18) T.G.1 Paris (ord. Réi), 22 Novembre 1984, D. 1984, Flash de jurisprudence, Nº 41.

(19) Le nouveau jeu interdit du week-end. Fabriquez-vous mêmes vu..e appareil à o décoder canal plus; BOUZAT (P.), obs. Sous Trib. Corr. Paris, 15 Avril 1985, F.S.C. 1987, P. 209, N° 1, R.T.D. Coin. 1987, 1. 259, 5, obs. BOUZAT (P.).

(20) BOUZAT (P.), obs. Sous CA. Paris, 24 Juin 1987, R.T.D. Com. 1988, p. B 298, Nº 2, le même auteur, obs. sous Trib. Corr. Paris, 15 Abril 1986, R.S.C, 1987, P. 210, N° 1, R.S.C. 1988, P. 794, N° 1; R.T.D. Com. 1987, P. 261, N° 2, obs. BOUZAT (P.).

المتعلقة بها.

وتتحقق هذه الهجمات من خلال التأثير المادي المباشر على الهدف، بما يؤدي إلى تقليل قيمته أو كفاءته في أداء الوظيفة التي صمم من أجلها، ويمكن فهمها ببساطة على أنها أفعال تؤدي إلى إضعاف أداء النظام أو أحد مكوناته أو التقليل من فعاليته(٢١).

قد تتعرض المواقع الحكومية للتخريب من خلال استخدام برامج مخصصة لنشر الفيروسات بداخلها، حيث تُزرع هذه الفيروسات في جزء معين من القرص الصلب أو المرن يُعرف بقطاع التحميل. وتمثل هذه النوعية من الفيروسات ما يقارب ٥% من إجمالي الفيروسات المعروفة التي تصيب أجهزة الحاسوب الشخصية، وتكمن خطورتها في أنها تبدأ بالعمل فور تشغيل الجهاز، نظراً لاحتواء هذا القطاع على التعليمات البرمجية التي تقوم بتحميل نظام التشغيل إلى الذاكرة(٢٢).

رابعًا- التحريض الإلكتروني على اختراق المواقع الإلكترونية الرسمية للدولة:

التحريض في هذا السياق يعني قيام شخص بدفع آخر أو التأثير عليه بطريقة تدفعه إلى ارتكاب الجريمة موضع الدراسة، سواء عن طريق إقناعه بالفكرة، أم تشجيعه، أم تهديده، أم تقديم إغراءات معينة. وقد يتم ذلك باستخدام وسائل تقنية متعددة، مثل المحادثات المباشرة، أو الرسائل المكتوبة، أو مقاطع الفيديو، أو الرسائل المرسلة عبر الإنترنت أو البريد الإلكتروني. كما يشمل هذا التحريض ما يتم تداوله أو نشره من خلال الوسائط الرقمية الحديثة مثل المواقع الإلكترونية، والهواتف الذكية، والمدونات، والملفات الإلكترونية، أو عن طريق مزودي خدمات الإنترنت(٢٣).

قد يصدر التحريض على اختراق المواقع الإلكترونية الرسمية من بعض العاملين في مجال الإنترنت، مثل مقدمي خدمات الاتصال، أو الجهات المستضيفة للمواقع، أو منتجي المحتوى، أو ناقلي البيانات، أو موردي المعلومات، أو حتى من يقوم بكتابة الرسائل الإلكترونية أو توفير الأدوات التقنية

---

(٢١) د. محمد الشهاوي، شرح قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣، ط١، دار النهضة العربية، القاهرة، ٢٠١٠م، ص١٩٩.

(٢٢) نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، ٢٠٠٨م، ص١٧٦ وما بعدها.

(٢٣) التحريض الإلكتروني، وزارة الداخلية المصرية، أكاديمية الشرطة، مركز بحوث الشرطة، الإصدار التاسع والأربعون، ٢٠١٤م، ص٣٥.

أو تقديم خدمات الدعم الفني. وتجدر الإشارة إلى أن عملية الدخول إلى شبكة الإنترنت غالبًا ما تعتمد على الاستعانة بمقدم خدمة اتصال، وهو الطرف المسؤول فنيًا عن تمكين المستخدم من الاتصال بالشبكة، حيث يتولى تشغيل الخادم المتصل بشكل دائم بالإنترنت، ويمنح المستخدم القدرة على تصفح المواقع، والدخول إلى الشبكة، والتواصل مع الآخرين، وتبادل الرسائل الإلكترونية(٢٤).

خامسًا- التجسس على المواقع الإلكترونية الرسمية للدولة:

يُقصد بالتجسس في هذا السياق محاولة الوصول إلى معلومات سرية تخص الدولة، تكون محفوظة داخل أجهزة خاصة ومؤمنة، ولا يُسمح لغير المصرح لهم بالاطلاع عليها. فقد أدى تطور الفضاء الإلكتروني إلى تغيير جذري في أساليب جمع المعلومات والتنصت، وسهّل من تنفيذ الأنشطة السرية المرتبطة بالعلاقات الدولية، مثل الاغتيالات، نتيجة ارتباط الأمن بشكل وثيق بالتكنولوجيا الحديثة.

وتسعى بعض الأجهزة الاستخباراتية إلى استقطاب القراصنة الإلكترونيين للاستفادة من مهاراتهم، سواء عبر التعاون مع شركات كبرى بهدف الحصول على معلومات عن منافسيها، أم من خلال توظيفهم لإلحاق الضرر بسمعة هذه الشركات والتأثير على ثقة العملاء بها. كما بات القراصنة أداة فعّالة في يد الجماعات المتطرفة، حيث يتم استخدامهم في التجسس ونشر أفكارهم عبر الإنترنت. بل وتلجأ بعض الدول إلى الاستعانة بهم في شن هجمات إلكترونية أو جمع معلومات عن دول أخرى تُعد خصمًا سياسيًا أو عسكريًا.

وفي ظل هذه التهديدات، يُعد التعامل مع هؤلاء القراصنة ضرورة أمنية قصوى، لا سيما مع صعوبة القضاء عليهم بشكل نهائي. لذلك، يُوصى بتكوين فرق متخصصة من الخبراء في المجال التقني لمجابهة هذا النوع من التجسس، خاصة وأن شبكة الإنترنت باتت وسيلة رئيسية لممارسة الأعمال التجسسية، سواء على الأفراد أو المؤسسات أم الدول، وتتنوع أهداف هذه العمليات بين أغراض عسكرية، أو سياسية، أو اقتصادية (٢٥).

---

(٢٤) د. جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي- الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ٢٠١٢م، ص١٣٣.

(٢٥) صباح كزيز، د. سمير قط، أثر الجرائم الإلكترونية على أمن واستقرار الدول: قرصنة الموقع الإلكتروني لوكالة =

سادسًا- اختراق المواقع الإلكترونية الرسمية للدولة:

- يتم ذلك بقصد تعريض الدولة للكثير من الأخطار:
- يُقصد بتعريض المجتمع والأمن للخطر إحداث أضرار تمس استقرار الدولة وتهدد سلامة مواطنيها، الأمر الذي يؤدي إلى اضطراب النظام العام. ومن الأمثلة الواضحة على ذلك، التلاعب بالأنظمة الإلكترونية الحساسة كأنظمة المرور أو شبكات السكك الحديدية، وهو ما قد يؤدي إلى توقف حركة القطارات أو تعطل حركة السير، مما ينشر حالة من الفوضى والقلق بين الناس، ويرفع من احتمالية وقوع حوادث تهدد حياة المواطنين بالخطر أو تؤدي إلى وفاتهم(٢٦).
- التسبب في أضرار بيئية وتهديد مصادر الحياة والزراعة، مثل التلاعب بالأنظمة الإلكترونية المسؤولة عن تشغيل وضخ المياه في السدود، مما قد يؤدي إلى تلف المحاصيل أو انقطاع المياه وإلحاق أذى كبير بالبيئة والإنسان(٢٧).
- يقصد بالإضرار بموارد الدولة الاقتصادية والتنموية التسبب في خسائر تؤثر سلبًا على استقرارها المالي ومسيرتها التنموية، ومن أبرز صور هذا الضرر، التلاعب بأرصدة البنوك والحسابات النقدية، حيث يتم تحويل الأموال إلى جهات غير معلومة، وهو ما يؤدي إلى فقدان الثقة في النظام المالي ويؤثر بشكل مباشر على الاقتصاد القومي للبلاد ويعرضه للخطر.(٢٨).
- شلّ عمل الأنظمة الإلكترونية المرتبطة بوسائل الاتصالات، وذلك بقصد التستر على أنشطة إجرامية، أو منع اكتشافها، أو حذف معلومات قد تسهم في كشف تفاصيل تلك الأفعال وملاحقة مرتكبيها(٢٩).

الأنباء القطرية أنموذجًا، مخبر أثر الاجتهاد القضائي على حركة التشريع- كلية الحقوق والعلوم السياسية، جامعة محمد خيضر- بسكرة، الجزائر، مجلة الناقد للدراسات السياسية، العدد الثالث، أكتوبر ٢٠١٨م، ص١٣٠.

(٢٦) د. موسى مسعود أرحومة، الإرهاب والإنترنت، مجلة دراسات وأبحاث، جامعة الجلفة – الجزائر، العدد الرابع، ٢٠١١م، ص١٧٧.

(٢٧) ماجد بن كريم الزارع، الركن المادي في الجرائم الإلكترونية في النظام السعودي – دراسة تأصيلية، رسالة ماجستير، جامعة نايف للعلوم الأمنية، الرياض، ٢٠١٤م، ص١٠٢.

(٢٨) المرجع السابق، الموضع نفسه.

(٢٩) ماجد بن كريم الزارع، الركن المادي في الجرائم الإلكترونية في النظام السعودي، دراسة تأصيلية، مرجع سابق،

- **تاسعًا**– ممارسة أي أعمال إلكترونية أخرى، من شأنها تعريض نظام الحكم في البلاد للخطر(٣٠):
- **عاشرًا**– ممارسة أي أعمال إرهابية من شأنها، التأثير أو تغيير الكيان الاقتصادي أو التأثير على التوافق المجتمعي، أو إحداث اضطراب في الأوضاع السياسية للمجتمع(٣١).

حادي عشر– انضمام المخترقين إلى مواقع التواصل الاجتماعي وغزوها:

ويُعزى ذلك إلى الدور الحيوي الذي تؤديه هذه المواقع في تحقيق أهدافهم المتنوعة، حيث تُستغل كوسيلة لنشر المعلومات المتعلقة بكيفية تصنيع القنابل وتنفيذ الهجمات، إضافة إلى تقديم إرشادات مفصلة للمُنضمين الجدد، كما تُستخدم في الترويج لأفكارهم والدعاية لأنشطتهم، وتُعد بمثابة قاعدة بيانات شاملة تحتوي على كل ما يخدم توجهاتهم وأهدافهم(٣٢).

مظاهر جريمة اختراق المواقع الإلكترونية:

ومن بين هذه الأساليب ما يُعرف بالقذف الإلكتروني، وهو الهجوم الذي يتم من خلال إرسال عدد كبير من الرسائل الإلكترونية دفعة واحدة إلى المواقع الرسمية التابعة للدولة، بقصد شل حركتها ومنعها من استقبال أي رسائل جديدة. وقد تعرضت العديد من المؤسسات الكبرى لهذا النوع من الهجمات، مما تسبب في حالة من القلق والخوف لدى الجمهور الذي يعتمد على خدمات تلك الجهات. وغالبًا ما يلجأ منفذو هذه الهجمات إلى إخفاء هويتهم باستخدام أسماء مستعارة وعناوين إلكترونية وهمية، الأمر الذي يصعب من مهمة تتبعهم أو الوصول إلى هويتهم الحقيقية(٣٣).

ص١٠٢.

(٣٠) عمر حوتية، وآخرون، تجربة دولة الإمارات في التصدي للجرائم المعلوماتية الواقعة على التجارة الإلكترونية – المجلة الأردنية للمكتبات والمعلومات – جمعية المكتبات والمعلومات الأردنية – الأردن، المجلد ٥٠ العدد ٤، كانون الأول ٢٠١٥م، ص١٤١.

(٣١) د. محمد قيراط: الإعلام الجديد والإرهاب الإلكتروني، آليات الاستخدام وتحديات المواجهة، مجلة الحكمة للدراسات الإعلامية والاتصالية – مؤسسة كنوز الحكمة للنشر والتوزيع – الجزائر، العدد التاسع، يناير ٢٠١٧م، ص٢٤ وما بعدها.

(٣٢) د. محمد قيراط، الإعلام الجديد والإرهاب الإلكتروني: آليات الاستخدام وتحديات المواجهة، موجع سابق، ص٢٥.

(٣٣) د. موسى مسعود أرحومة، الإرهاب والإنترنت، مرجع سابق، ص١٧٨.

ومن الجدير بالذكر أن هذه الأنواع من الجرائم الإلكترونية تُسبب خسائر مالية فادحة، حيث تتحمل الدول أعباء اقتصادية كبيرة نتيجة تزايد هذه الهجمات الرقمية، وبشكل خاص تلك التي تستهدف المواقع الرسمية التابعة للدولة. وقد تصل قيمة هذه الخسائر إلى مئات المليارات من الدولارات، مما يوضح التأثير العميق والخطير لمثل هذه الجرائم على الاستقرار المالي والاقتصادي [٣٤]، فإنه طبقًا لتقرير صادر عن مركز الدراسات الاستراتيجية والدولية (CSIS)[٣٥] والصادر عام ٢٠١٤م، فإن هذه الجرائم تؤدي إلى خسارة تقدر بنحو ٤٤٥ مليار دولار كل عام[٣٦].

وبصورة عامة، فإن أي فعل إلكتروني يهدف إلى ارتكاب الجريمة محل البحث بغرض الإضرار بأمن المجتمع واستقراره، وما يترتب عليه من تهديد للنظام العام، يُعد من مكونات الجانب المادي للجريمة، سواء تم ارتكابه فعليًا أم اقتصر الأمر على مجرد التهديد به. وقد أكدت المحكمة الاتحادية العليا على أهمية معاقبة كل من يستخدم الإنترنت أو وسائل الاتصالات في بث الخوف والذعر، أو في التسبب بأذى نفسي للآخرين، أو في إزعاجهم لتحقيق أغراض لا يجيزها القانون [٣٧].

محل جريمة اختراق المواقع الإلكترونية:

الغاية الأساسية من جريمة اختراق المواقع الإلكترونية تتمثل في ما تتركه من تأثير نفسي واجتماعي، حيث تنشر مشاعر الخوف والذعر وتثير القلق بين الناس. وهذا التأثير وحده يُعد كافيًا لاعتبار العنصر المادي للجريمة متحققًا، حتى وإن لم يقع ضرر فعلي، إذ يكفي وجود احتمال منطقي لحدوثه. وبناءً على ذلك، تُعد هذه الجريمة من "جرائم الخطر" التي يُعاقب فيها القانون على القصد

---

(34) First Annual Cost of Cyber Crime Study, Peneman Institute, Research Report MI. 2010, p. 63.

(٣٥) مركز الدراسات الاستراتيجية والدولية (CSIS)، هو مركز أبحاث سياسية أمريكي مقره واشنطن دي سي، بالولايات المتحدة، تأسس "كمركز للدراسات الاستراتيجية والسياسية"، في جامعة جورجتاون عام ١٩٦٢م، يقوم المركز بعقد دراسات سياسية وتحليل استراتيجي للقضايا السياسية، الاقتصادية والأمنية في جميع أنحاء العالم، مع التركيز بشكل خاص على القضايا المتعلقة بالعلاقات الدولية، التجارة، التكنولوجيا، المالية، الطاقة". (https://www.marefa) تم زيارة الموقع يوم الجمعة الموافق ٢٠٢١/٧/٢٧م، في تمام الساعة السابعة مساءً.

(٣٦) عمر حوتية، وآخرون، تجربة دولة الإمارات في التصدي للجرائم المعلوماتية الواقعة على التجارة الإلكترونية، مرجع سابق، ص١٤٩.

(٣٧) دولة الإمارات العربية المتحدة: المحكمة الاتحادية العليا، دائرة الأحكام المدنية والتجار، الطعن رقم١، لسنة ٢٠١٥ ق، بتاريخ ٢٠١٥/٦/١٦م.

والسلوك، دون أن يشترط حدوث نتيجة ضارة بشكل فعلي [٣٨]، بل إن بارتكاب النشاط الإجرامي الذي يراد به تحقيق النتيجة – نفسيًا او ماديًا – فيمكن القول بتوافر الركن المادي، وعلى ذلك فإن تحقق الغرض من هذا السلوك قائم، وتحقق الرعب مرتبط بتحقق الفعل[٣٩].

المطلب الثاني

النتيجة في جريمة اختراق المواقع الإلكترونية

تجسد النتيجة العنصر الثاني من عناصر الركن المادي، ويقصد بها الأثر المترتب على السلوك الإجرامي، والذي يأخذه المشرع بعين الاعتبار في التكوين القانوني للجريمة، فالركن المادي للجريمة يتكون من السلوك الإجرامي، سواء كان سلوكًا إجراميًا أم سلبيًا، والآثار المترتبة عليه، واللازمة للوجود القانوني للجريمة، وهي النتيجة الإجرامية[٤٠]، وهي– كذلك– تمثل الآثار المترتبة ارتكاب الجاني لسلوكه الإجرامي، أو يمكن القول بأنها العدوان بصورته النهائية على المصلحة التي يحميها القانون[٤١]، ومن ثم فهي الأثر الطبيعي الناتج عن النشاط الإجرامي، والذي يعتد به القانون[٤٢].

يمكن القول إن النتيجة الإجرامية تُجسد الأثر الملموس الذي ينشأ عن الفعل الذي يجرّمه القانون، وهي النتيجة المباشرة المترتبة على التصرف الإجرامي. وبناءً على ذلك، لا يمكن تحميل الجاني مسؤولية عن نتائج لم تكن مرتبطة ارتباطًا مباشرًا بسلوكه، إذ يشترط وجود علاقة سببية واضحة بين الفعل الذي ارتكبه والنتيجة التي حدثت [٤٣].

---

(٣٨) د. معن أحمد الحياري، الركن المادي للجريمة، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠١٠م، ص٢٠٩.

(٣٩) ماجد بن كريم الزارع، الركن المادي في الجرائم الإلكترونية في النظام السعودي دراسة تأصيلية، مرجع سابق، ص١٠٣.

(٤٠) د. طلعت الشهاوي، المسئولية الجنائية عن جرائم الاتصالات – دراسة مقارنة مع قوانين الاتصالات في فرنسا والولايات المتحدة الأمريكية والمملكة العربية السعودية والإمارات وقطر وليبيا وتونس ولبنان والكويت وسلطنة عمان والسودان وسوريا والأردن وفلسطين والبحرين، دار النهضة العربية، القاهرة، ٢٠١٩م، ص٩٣ وما بعدها.

(٤١) د. علي محمود علي حموده، النظرية العامة في تسبيب الحكم الجنائي في مراحله المختلفة – دراسة مقارنة"، رسالة دكتوراه، القاهرة، ١٩٩٤م، ص٢٩١.

(٤٢) د. محمد عبد اللطيف عبد العال، النظرية العامة للجريمة والمسؤولية الجنائية في القانون الكويتي، مجلس النشر العلمي، جامعة الكويت، ٢٠١٥م، ٣٣٤.

(٤٣) د. أحمد المجدوب، التحريض على الجريمة، دراسة مقارنة، بدون رقم طبعة، الهيئة العامة لشئون المطابع =

في جريمة التسلل إلى المواقع الرسمية التابعة للدولة، تظهر النتائج الإجرامية من خلال التسبب بخلل في أنظمة الدولة، أو تدمير بعض مكوناتها الإلكترونية، أو اختراقها بقصد الحصول على معلومات سرية، أو زعزعة استقرار النظام الحاكم. وقد بيّن القانون الاتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الإلكترونية خطورة هذه التصرفات، حيث نصت المادة (٧١) منه على أن الجرائم الواردة في المواد (٣، ٥، ٧، ١١ فقرة ٣، ١٢ فقرة ٣، ١٣، ١٩، ٢٠، ٢١، ٢٣، ٢٤، ٢٥، ٢٦، ٢٧، ٢٨، ٤٧ فقرة ثانية، ٥٢، ٥٣، ٥٥) تُعتبر من الأفعال التي تمس بأمن الدولة، وتندرج ضمن الجرائم الرقمية، مما يوضح بجلاء أن جريمة اختراق المواقع الإلكترونية الرسمية تُعد من أخطر الجرائم التي تمس أمن الدولة.(٤٤)

كما تُصنف ضمن هذا النوع من الجرائم أيضاً كل جريمة ورد النص عليها في هذا القانون إذا تم ارتكابها لصالح أو لحساب جهة أجنبية أو جماعة إرهابية أو منظمة أو كيان غير قانوني(٤٥).

تترتب على النتيجة الإجرامية آثار قانونية بالغة الأهمية، خصوصاً من حيث ارتباطها بالقصد الجنائي، حيث إن تحقق هذه النتيجة يُعد مبرراً لتشديد العقوبة المقررة للجريمة. وبناءً عليه، تُفهم النتيجة الإجرامية في الجانب المادي لجريمة اختراق المواقع الإلكترونية على أنها تمثل اعتداءً على مصلحة معينة يعتبرها المشرّع الإماراتي جديرة بالحماية ضمن إطار القانون الجنائي(٤٦).

وفي الغالب، تُعد النتيجة الإجرامية واقعًا ماديًا ملموسًا، يظهر في صورة ضرر فعلي يترك أثره في العالم الخارجي (٤٧)،مثل تخريب أحد الأنظمة الإلكترونية الرسمية للدولة، وذلك بقصد التستر على أنشطة غير قانونية تُلحق الأذى بمصالح الدولة.

الأميرية، القاهرة، ١٩٨٧م، ص٣٩٣.

(٤٤) وهو ما نص عليه القانون رقم (٥) لسنة ٢٠١٢م بشأن مكافحة جرائم تقنية المعلومات الإماراتي الملغي، وذلك في المادة (٤٤) منه، والتي اعتبرت أن صور الجرائم الواردة في المواد (٤، ٢٤، ٢٦، ٢٨، ٢٩، ٣٠، ٣٨) من القانون نفسه، هي من الجرائم الماسة بأمن الدولة، وهي من حيث الأصل جرائم إلكترونية.

(٤٥) راجع في ذلك الفقرة الثانية من المادة (٧١) من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الإلكترونية.

(٤٦) د. محمود نجيب حسني، شرح قانون العقوبات– القسم العام، مرجع سابق، ص٥٠٩.

(٤٧) د. عبود السراج، قانون العقوبات– القسم العام، منشورات جامعة حلب، سوريا، ١٩٩٧م، ص١٩٣.

تُعد طبيعة المصلحة التي يُراد حمايتها نقطة محورية لدى المشرع في كل من الإمارات ومصر عند تحديد النتيجة الإجرامية؛ إذ يرى المشرع أن هناك مصالح تتطلب الحماية لمجرد تعرضها للتهديد، حتى وإن لم تُحدث الأفعال الإجرامية نتائج مادية ملموسة. وفي المقابل، توجد مصالح وحقوق أخرى لا تُمنح الحماية إلا إذا نتج عن السلوك الإجرامي تأثير فعلي ملموس، يظهر من خلال آثار مادية واقعة[٤٨].

وبناءً على ما سبق، يمكن القول إن النتيجة تُجسّد اعتداءً صريحًا على المصالح التي كفل لها القانون الحماية، أو تُعبّر عن تعارض مع القيم والمبادئ السائدة في المجتمع، وتمثل تعديًا على حريات الأفراد وتصرفاتهم القانونية. وتتحقق النتيجة بمجرد وقوع الفعل الإجرامي، المتمثل في انتهاك القوانين أو مخالفة التعليمات التي يجب الالتزام بها. أما الأثر المتوقع من جريمة اختراق المواقع الإلكترونية ، فهو زعزعة وضع الجهة المستهدفة، سواء كانت الدولة نفسها أم أحد مكوناتها الرسمية، وكذلك تهديد المجتمع باعتباره المتضرر من هذا الفعل. وقد يبدأ الجاني بتنفيذ هذه الجريمة ثم يتوقف قبل الشروع الفعلي فيها أو قبل استكمال أركانها، كما قد يتراجع عن الاستمرار في نشاطه ويكفّ عن اختراق تلك المواقع[٤٩].

---

(٤٨) المرجع السابق، ص٢٩٠.

(٤٩) د. محمد الحديثي، جرائم التحريض وصورها في الجوانب الماسة بأمن الدولة الخارجي وفقًا للتشريع العراقي، مطابع وزارة الثقافة والإعلام، بغداد، ١٩٨٤م، ص١٧٧.

وعلى ما تقدم، يتضح لنا أن النتيجة الإجرامية، يقصد بها أحد المفهومين الآتيين[٥٠]:

المفهوم القانوني: يُستخدم هذا المفهوم عندما يتم التعدي على حق أو مصلحة يحميها القانون الجنائي، سواء وقع الضرر بشكل فعلي، أم اقتصر الأمر على تهديد تلك المصلحة بالخطر. وبهذا المعنى، فإن النتيجة تظل ملازمة لأي فعل جرمي، وتعبر عن السبب الذي من أجله جُرّم السلوك في الأساس. أي أن النتيجة ليست منفصلة عن الفعل نفسه، بل هي مرتبطة به ارتباطًا وثيقًا. ومن هنا، فإن حتى الجرائم التي لم تُستكمل (أي الشروع) يُنظر إليها على أن لها نتيجة قائمة، وهي ما ينجم عن هذا السلوك من تهديد حقيقي للمصلحة المحمية[٥١].

المفهوم المادي: النتيجة هنا تشير إلى الأثر الذي يتركه الفعل الإجرامي في الواقع الخارجي، بحيث يعترف به قانون العقوبات ويعتبره أساسًا للمساءلة. في هذا السياق، تكتسب النتيجة وجودًا ماديًا منفصلًا عن الفعل نفسه، مثل نشر الخوف والقلق بين الناس، أو الدعوة عبر الإنترنت لأعمال عنف ضد الدولة. ويُعد هذا المفهوم هو الأكثر شيوعًا في قوانين العقوبات، خاصة في الأنظمة الليبرالية التي تركز على منع وقوع الاضطراب في المجتمع. ويُنظر عادةً إلى التغير الملموس الناتج عن الفعل الإجرامي كمؤشر على جسامة الجريمة، وغالبًا ما يتم تحديد مقدار العقوبة بناءً على حجم هذا الضرر الملموس[٥٢].

يُعتبر عنصر النتيجة في الجانب المادي لجريمة اختراق المواقع الإلكترونية من العناصر المعقدة، نظرًا لصعوبة إثباته، نتيجة للطبيعة الخاصة التي تتميز بها الجرائم الإلكترونية وتعدد النتائج التي قد تترتب عليها. فقد لا تظهر النتيجة مباشرة بعد ارتكاب الجريمة، بل قد يستغرق الأمر وقتًا حتى تتضح آثار الفعل، ويتباين هذا التأخير بحسب حجم الأثر الذي خلّفه الاختراق، ويختلف من حالة إلى أخرى. كما يمكن أن تقع النتيجة في نفس مكان ارتكاب الفعل، أو في مكان آخر تمامًا، مثلما يحدث في

---

(٥٠) د. حسن محمد ربيع، شرح قانون العقوبات الاتحادي، ط١، أكاديمية شرطة دبي، الإمارات العربية المتحدة، ٢٠٠٦م، ص٢٢٠.

(٥١) د. مأمون محمد سلامة، قانون العقوبات القسم العام، مطبعة جامعة القاهرة والكتاب الجامعي، القاهرة، ١٩٩٦م، ص١٣٩.

(٥٢) د. أحمد شوقي عمر أبو خطوة، شرح الأحكام العامة لقانون العقوبات، دار النهضة العربية، القاهرة، ٢٠٠٠م، ص١٧٦.

حالات التحريض على اختراق أو تخريب مواقع الدولة، حيث يتم التحريض من جهة، بينما تُنفذ الجريمة في جهة مختلفة. وفي بعض الحالات، لا تكون هناك نتيجة مادية واضحة، وإنما يكفي أن تُعرض البيانات الرقمية للدولة للخطر ليُعتبر ذلك نتيجة قانونية تترتب عليها آثار ملموسة[٥٣].

يتبيّن من أسلوب تعامل المشرعين في كل من الإمارات ومصر مع الجريمة محل البحث، أنهم يهدفون إلى تأمين المؤسسات والجهات الحكومية التي قد تتعرض لمثل هذه الأفعال، وذلك عبر تجريم أي سلوك قد يُمثل تهديداً لها، حتى في حال عدم وقوع ضرر مباشر. ويعكس هذا التوجه انسجاماً مع ما تنص عليه العديد من التشريعات الأخرى التي تتصدى للجرائم الإلكترونية بأسلوب وقائي يركز على منع الخطر قبل وقوعه.

كما أن المشرع الإماراتي لا يعتبر جريمة اختراق المواقع الرسمية من جرائم الخطر بهدف التوسع في العقاب، بل من منطلق حماية المصالح التي قد تتعرض للاستهداف، حتى إن اقتصر الأمر على مجرد التهديد دون أن يتحقق ضرر فعلي. ومع ذلك، توجد حالات معينة لا تُعد فيها الأفعال جريمة إلا إذا ترتب عليها ضرر محدد، وهو ما ينطبق على بعض الجرائم الأخرى أيضاً. ومن خلال ذلك، يتضح أن عنصر النتيجة في جريمة اختراق المواقع يتوافق مع القواعد العامة، إذ يشترط المشرع في بعض المواقف حدوث ضرر حقيقي، بينما في مواقف أخرى يكتفي بحدوث السلوك المحظور إذا كان من شأنه تعريض مصالح معينة للخطر. وفي هذه الحالة، يصبح التهديد وحده نتيجة قانونية كافية لتوقيع العقوبة، بهدف الحيلولة دون تفاقم الأمور ووقوع ضرر فعلي لاحق. وتتمثل النتيجة الإجرامية في هذه الجريمة فيما يترتب على السلوك المحظور من آثار واضحة، حيث تتحقق هذه النتيجة بمجرد إقدام الجاني على فعل يجرّمه القانون. فوفقاً للمرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الإلكترونية، لم يُشترط تحقق ضرر فعلي حتى تُعد الجريمة قائمة، بل يكفي ارتكاب الفعل الممنوع لاعتبار النتيجة متحققة، وبالتالي تطبيق العقوبة القانونية[٥٤]،وكذلك لم يشترط المشرع المصري، في القانون رقم (١٧٥) لسنة ٢٠١٨ بشأن مكافحة

---

(٥٣) د. عادل عبد الصادق، الفضاء الإلكتروني والعلاقات الدولية– دراسة في النظرية والتطبيق، ط١، المكتبة الأكاديمية، القاهرة، ٢٠١٦م، ص١٣٧.

(٥٤) وكذلك الحال في مواد المرسوم بقانون رقم (٥) لسنة ٢٠١٢م الملغي.

جرائم تقنية المعلومات، توافر شروط محددة لوقوع النتيجة الإجرامية حتى يمكن القول بقيام المسؤولية الجنائية، بل ترك تقدير تحقق هذه النتيجة لسلطة القاضي التقديرية، وفقًا لما يتوافر لديه من وقائع وظروف كل حالة على حدة(٥٥).

بناءً على ذلك، فإن الأثر الناتج عن جريمة اختراق المواقع الإلكترونية يتمثل في الأذى الذي يُلحقه الفاعل نتيجة استخدامه أدوات إلكترونية للتسلل إلى هذه المواقع، مما يؤدي إلى تهديد أمن المجتمع أو زعزعة استقراره. ويكفي في هذه الحالة أن يكون هناك احتمال لحدوث هذا الضرر، دون الحاجة لوقوعه فعلاً، طالما أن الأمر يثير الخوف والقلق لدى الناس(٥٦).

تظهر النتيجة الإجرامية لاستخدام الإنترنت في اختراق المواقع الرسمية للدولة عندما يقوم الفرد بإنشاء مواقع أو صفحات إلكترونية تُستخدم كوسيلة للتواصل مع هذه المواقع، أو لنشر أفكار تتعلق بعمليات الاختراق والتشفير، أو بتقديم تمويل يدعم هذه الأفعال، أو حتى بنشر أدوات وبرامج تُستخدم في تنفيذ الاختراق. وتتحقق هذه النتيجة بمجرد نشر أو عرض تلك الوسائل أو المعلومات التي تعين على تنفيذ الجريمة، سواء بشكل مباشر أم غير مباشر، حتى في حال عدم ظهور أي أثر مادي واضح، إذ إن مجرد نشر طريقة إعداد أدوات الاختراق يُعد فعلًا مجرمًا بذاته، ولا يتطلب الأمر وقوع ضرر فعلي لإثبات الجريمة (٥٧)،لا يُشترط في جريمة اختراق المواقع الإلكترونية أن يترتب عليها ضرر فعلي، فهي تُعد من الجرائم الشكلية التي تكتمل بمجرد قيام الشخص بالفعل المجرّم. فالمشرّع لم يشترط وقوع نتيجة ملموسة لتوقيع العقوبة، باعتبار أن مثل هذه الأفعال تمثل تهديدًا لأمن الدولة واستقرارها ومصالحها العامة، حتى وإن لم تُحدث أثرًا مباشرًا (٥٨).

---

(٥٥) ماجد بن كريم الزارع، الركن المادي في الجرائم الإلكترونية في النظام السعودي، مرجع سابق، ص١٦٤.

(٥٦) حسن بن محمد السلطان، تجريم تمويل الإرهاب والعقاب عليه– دراسة تحليلية مقارنة، رسالة ماجستير، جامعة نايف للعلوم الأمنية، الرياض، ٢٠٠٩م، ص٤٣.

(٥٧) ماجد بن كريم الزارع، الركن المادي في الجرائم الإلكترونية في النظام السعودي، دراسة تأصيلية، مرجع سابق، ص١٦٤

(٥٨) د. معن أحمد الحياري، الركن المادي للجريمة، مرجع سابق، ص١٩٥.

المطلب الثالث

علاقة السببية بين الفعل والنتيجة في

جريمة اختراق المواقع الإلكترونية

تعني علاقة السببية وجود رابط مباشر وواضح بين الفعل الذي قام به الجاني والنتيجة التي ترتبت على هذا الفعل، ويُشترط أن تكون هذه العلاقة خالية من االلتباس، لأنها تشكّل الأساس الذي يقوم عليه الجانب المادي للجريمة. وبعبارة أخرى، يجب أن يكون سلوك الجاني هو السبب الفعلي والمباشر لوقوع النتيجة الإجرامية، بحيث يمكن إسنادها إليه بشكل قاطع [٥٩]،لا يُحاسب الجاني على نتيجة فعله الإجرامي إلا إذا وُجد ارتباط سببي بين هذا الفعل والنتيجة التي ترتبت عليه. فإذا كانت هذه العلاقة قائمة، أمكن تحميله المسؤولية عن النتيجة التي وقعت. أما إذا لم تكن هناك صلة بين الفعل والنتيجة، أو إذا انقطعت هذه العلاقة قبل وقوع النتيجة، ففي هذه الحالة يُحاسب الجاني على الفعل الذي ارتكبه فقط، دون أن يُحمّل تبعات النتيجة التي لم تكن ناتجة عنه بشكل مباشر[٦٠].

تُعتبر علاقة السببية من العناصر القانونية الأساسية، فهي تمثل الصلة التي تربط بين الفعل الإجرامي والنتيجة المترتبة عليه ضمن مكونات الركن المادي للجريمة، ما يجعل هذا الركن مكتملًا، ويُتيح إسناد النتيجة إلى التصرف الذي صدر عن الجاني. وتشكل هذه العلاقة شرطًا ضروريًا لتحميل الجاني تبعات النتيجة، كما أنها تحدد نطاق مسؤوليته. ففي حال غياب هذه العلاقة، لا يُسأل الفاعل عن النتيجة، بل تُقتصر مسؤوليته على مجرد محاولة ارتكاب الجريمة في الحالات العمدية. أما في الجرائم غير العمدية، فإن انعدام علاقة السببية يعفيه من المسؤولية تمامًا، لأن القانون لا يُقر بمسألة الشروع فيها. ولهذا، فإن علاقة السببية تُعد عنصرًا جوهريًا في الركن المادي للجريمة، ولا يمكن قيام المسؤولية الجنائية بدونها[٦١].

بينما يُنظر إلى مفهوم السببية في العلوم على أنه ارتباط مباشر وثابت بين حدثين يحدث بشكل

---

(٥٩) د. محمود نجيب حسني، شرح قانون العقوبات – القسم العام، مرجع سابق، ص ٣٨٨.

(٦٠) د. أحمد شوقي عمر أبو خطوة، شرح الأحكام العامة لقانون العقوبات، مرجع سابق، ص٢١٦.

(٦١) خالد بن محمد سليمان المرزوق، جريمة الاتجار بالنساء والأطفال وعقوباتها في الشريعة الإسلامية والقانون الدولي – دراسة تأصيلية مقارنة، رسالة ماجستير، جامعة نايف للعلوم الأمنية، الرياض، ٢٠٠٥م، ص٨٨.

منتظم، فإن المعنى القانوني يختلف في طبيعته، حيث يركز على ما إذا كان يمكن اعتبار الفعل الذي قام به الجاني سبباً في وقوع النتيجة التي تلت ذلك، أي التحقق من مدى إمكانية نسب هذه النتيجة إلى ذلك الفعل. ويُلاحظ أن تصرفات الإنسان تحمل طابعًا خاصاً يميزها عن غيرها من الكائنات، مما يجعل من الصعب قياسها أو اختبارها بالطريقة نفسها المستخدمة في العلوم الطبيعية، خاصة وأن السلوك الإنساني يتأثر بعدة عوامل وظروف متغيرة. وتكمن أهمية علاقة السببية في القانون في كونها العنصر الذي يربط الفعل بالنتيجة داخل إطار الركن المادي للجريمة، فهي التي تمنح هذا الركن تماسكه وتكامله، وتجعله وحدة مترابطة ومتجانسة في بنيته القانونية (٦٢).

يقوم معيار علاقة السببية على فكرة أن الجرائم لا تنتج دائماً عن فعل واحد فقط، سواء أكان هذا الفعل إيجابياً أم سلبياً، بل قد تتداخل عدة تصرفات في إحداث النتيجة الإجرامية. فقد تكون هناك أفعال سبقت الفعل الرئيسي، أو وقعت في نفس الوقت، أو حتى لحقت به، ويمكن أن تسهم هذه الأفعال كلها أو بعضها في الوصول إلى النتيجة. كما قد تتحقق النتيجة بفعل واحد فقط دون الحاجة إلى تدخل باقي الأفعال(٦٣).

لا تُشكل مسألة إثبات علاقة السببية في جريمة اختراق المواقع الإلكترونية تحدياً كبيراً عندما ينتج عن فعل الجاني أثر مباشر وفوري يُفضي إلى النتيجة الإجرامية. غير أن الصعوبة تظهر عندما تتأخر هذه النتيجة في الظهور، أو تحدث في وقت ومكان يختلفان عن زمان ومكان الفعل الأصلي. وتزداد الأمور تعقيداً عندما تتداخل عدة عوامل في إحداث النتيجة، مما يتطلب تحديد السبب الذي يمكن تحميله وحده مسؤولية وقوع الجريمة، وهو ما يجعل إثبات السببية أكثر دقة وتعقيداً في هذه الحالات(٦٤).

في الجريمة محل البحث، لا بد أن يكون السلوك الذي ارتكبه الجاني هو العامل الرئيسي في وقوع النتيجة الإجرامية، بحيث توجد علاقة سببية واضحة ومباشرة تربط بين الفعل المرتكب والنتيجة

---

(٦٢) د. محمود نجيب حسني، علاقة السببية في قانون العقوبات، طبعة نادي القضاة، القاهرة، ١٩٨٤م، ص٥.

(٦٣) د. سوزي عدلي ناشد، الإرهاب الإلكتروني بين الاقتصاد الخفي والاقتصاد الرسمي، ط١، دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠٥م، ص٧٣.

(٦٤) د. محمود نجيب حسني، شرح قانون العقوبات – القسم العام، مرجع سابق، ص٣٩٤؛ مأمون محمد سلامة، قانون العقوبات – القسم العام، مرجع سابق، ص١٣٥.

التي تحققت بالفعل. وتشمل هذه الأفعال، على سبيل المثال، إنشاء موقع إلكتروني يُستخدم في تنفيذ عملية الاختراق، أو نشر معلومات وبيانات تتصل بالجريمة، أو عرض طرق وأساليب تساعد في تعليم الاختراق والتشفير، أو تقديم أي نوع من الدعم الذي يمكّن الآخرين من تنفيذ الهجوم. ويُشترط أن يكون هذا السلوك مرتبطًا بشكل مباشر بالنتيجة التي قصد الجاني الوصول إليها، دون تدخل مؤثرات خارجية تقطع هذا الترابط. وإذا انقطعت هذه العلاقة، فلا يمكن تحميل الجاني كامل المسؤولية عن جريمة اختراق المواقع الإلكترونية الرسمية(٦٥).

وبناءً على ما سبق، فإن تحقق الركن المادي في جريمة اختراق المواقع الإلكترونية يتطلب أن يصدر عن الجاني فعل إجرامي، سواء تم باستخدام وسيلة قانونية أم غير قانونية، ويؤدي هذا الفعل في نهايته إلى تنفيذ عملية الاختراق. كما يجب أن تترتب على هذا السلوك نتيجة مباشرة، مع وجود علاقة سببية واضحة تربط بين الفعل المرتكب والنتيجة التي تحققت، إذ لا تُعد الجريمة قائمة ما لم تجتمع هذه العناصر الثلاثة معًا.

المبحث الثاني

الركن المعنوي في جريمة اختراق المواقع الإلكترونية

تمهيد وتقسيم:

يُشترط لقيام الركن المعنوي في جريمة اختراق المواقع الإلكترونية وجود القصد الجنائي العام، أي أن تتجه إرادة الجاني إلى ارتكاب الفعل الإجرامي، وهو على علم بحقيقته وبما ينطوي عليه من مخالفة للقانون. ولا يشترط في هذه الجريمة توافر نية خاصة أو دافع معين، إذ تُعد جريمة مستقلة يُعاقب عليها القانون بمجرد تحقق القصد العام، سواء كانت لدى الجاني نية محددة أم غرض خاص أم لا(٦٦).

وبالتالي، فإن النية الإجرامية تُشكل الأساس الذي يقوم عليه العنصر المعنوي في جريمة

---

(٦٥) ماجد بن كريم الزارع، الركن المادي في الجرائم الإلكترونية في النظام السعودي، دراسة تأصيلية، مرجع سابق، ص١٦٥.

(٦٦) إبراهيم عبد الخالق، الشامل في جرائم الإنترنت في ضوء قانون العقوبات، المكتب الفني للإصدارات القانونية، القاهرة، ٢٠٢١م، ص٧٦.

اختراق المواقع الإلكترونية ويتحقق هذا العنصر عندما يكون الفاعل واعيًا تمامًا بما يقوم به، ويُدرك الجوانب القانونية للفعل الذي ارتكبه، ويعلم بالعواقب المحتملة المترتبة عليه. ويُعتبر هذا القصد عاملًا حاسمًا في تقدير العقوبة، حيث تختلف شدة الجزاء تبعًا لمدى وعي الجاني وإرادته أثناء ارتكاب الفعل.

كما أن تحقق القصد يستلزم أن تتجه إرادة الفاعل إلى القيام بالفعل الإجرامي وتحقيق الغاية المرجوة منه. ويُقاس مدى تحقق العلم من خلال شمول المعرفة لجميع عناصر الجريمة، أما ما يتجاوز حدود تلك العناصر، فلا يُعتد به. ويُفترض علم الجاني بنتيجة فعله، ولا يُقبل منه التذرع بالجهل كوسيلة للإفلات من المسؤولية.

المطلب الأول

القصد الجنائي العام

عرّف الفقيه الفرنسي جاريسون القصد الجنائي بأنه تعمّد الشخص ارتكاب الفعل المجرّم كما حدده القانون، أي أن يكون الجاني مدركًا تمامًا أنه يقوم بخرق قاعدة قانونية عند ارتكابه لذلك الفعل. وهذا الإدراك يُفترض وجوده لدى الجاني، ولا يُمكنه التذرع بالجهل بالقانون كوسيلة للإفلات من المسؤولية[٦٧]، ويعرِّفه البعض بأنه: العلم بعناصر الجريمة وإرادة متجهة إلى تحقيق هذه العناصر أو قبولها[٦٨].

القصد الجنائي العام يُقصد به توجه إرادة الشخص، مع علمه، إلى القيام بالفعل أو الامتناع عنه، متى كان هذا الفعل مخالفًا للقانون. فالعلم والإرادة هما العنصران الأساسيان في تكوين هذا القصد. ويتحقق العمد عندما يكون لدى الجاني رغبة في تنفيذ السلوك الإجرامي بهدف الوصول إلى نتيجة معينة يُعاقب عليها، أو حتى إذا توقع حدوث نتيجة أخرى غير مقصودة لكنها مخالفة للقانون، وكان مستعدًا لتحملها[٦٩].

---

(٦٧) د. جرجس جرجس، معجم المصطلحات الفقهية والقانونية، مراجعة: القاضي انطوان الناشف، ط١، الشركة العالمية للكتاب، بيروت – لبنان، ١٩٩٦م، ص٥١٤.

(٦٨) د. محمود نجيب حسني، شرح قانون العقوبات – القسم العام، مرجع سابق، ص ١٠٤.

(٦٩) د. غنام محمد غنام، الوجيز في شرح قانون العقوبات – القسم العام، ط١، مطبعة جامعة المنصورة الجديدة، المنصورة – مصر، ٢٠٠٨م، ص١٩٧.

القصد الجنائي العام في القانون الإماراتي يتحقق عندما تتجه إرادة الشخص إلى القيام بفعل أو الامتناع عنه، إذا كان هذا التصرف مخالفًا للقانون، ويكون الهدف من وراء ذلك إحداث نتيجة يعاقب عليها القانون، سواء كانت هذه النتيجة مقصودة بشكل مباشر، أم نتيجة أخرى كان الجاني يتوقع حدوثها. وقد ورد في النص القانوني أن العمد يقوم على توافر نية الجاني في تنفيذ الفعل أو الامتناع عنه، إذا كان هذا السلوك مجرماً، وكانت لديه نية في تحقيق نتيجة مباشرة أو أي نتيجة أخرى مجرّمة كان يتوقعها(٧٠).

لم يقم المشرع المصري بتحديد معنى القصد الجنائي بشكل مباشر في قانون العقوبات، بينما يرى الباحث أن المشرع الإماراتي قد اتخذ خطوة موفقة عندما قام بتحديد هذا المفهوم بوضوح، كما فعلت بعض القوانين الأخرى. ويعتقد الباحث أن تحديد ما إذا كان القصد الجنائي متوفراً أم لا يتطلب الرجوع إلى نصوص القانون، حيث يوضح المشرع ذلك من خلال استخدام بعض العبارات مثل "العمد". كما أن المشرع المصري استخدم تعبيرات متعددة تدل على القصد مثل "يقصد" و"بقصد" في عدد كبير من مواد قانون العقوبات، تجاوزت الستين موضعًا (٧١)، وهو ما نبينه على النحو الآتي:

---

(٧٠) كما عرفت المادة الأولى من القانون الاتحادي رقم (٧) لسنة ٢٠١٤م بشأن مكافحة الجرائم الإرهابية القصد أو الغرض الجنائي بأنه: "اتجاه إرادة الجاني إلى ارتكاب فعل أو الامتناع عن فعل، متى كان هذا الارتكاب أو الامتناع وذلك بقصد إحداث نتيجة إرهابية ً قانونًا مجرما مباشرة أو غير مباشرة أو علم الجاني بأن من شأن الفعل أو الامتناع عن الفعل، تحقيق نتيجة إرهابية"

(٧١) من ذلك ما نصت عليه المادة (٨٠) (١)؛ حيث نصت على أن: " يعاقب بالإعدام كل من سلم لدولة أجنبية أو لأحد ممن يعملون لمصلحتها أو أفشي إليها أو إليه بأية صورة وعلى أي وجه وبأية وسيلة سرا من أسرار الدفاع عن البلاد أو توصل بأية طريقة إلى الحصول على سر من هذه الأسرار بقصد تسليمه أو إفشائه لدولة أجنبية أو لأحد ممن يعملون لمصلحتها وكذلك كل من أتلف لمصلحة دولة أجنبية شيئًا يعتبر سرً□ا من أسرار الدفاع أو جعله غير صالح لأن ينتفع به"، والمادة (٨٠) (أ)، والتي نصت على أن: "يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على خمس سنوات وبغرامة لا تقل عن ١٠٠ جنيه ولا تجاوز ٥٠٠ جنيه. ١. كل من حصل بأية وسيلة غير مشروعة على سر من أسرار الدفاع عن البلاد ولم يقصد تسليمه أو إفشاءه لدولة أجنبية أو لأحد ممن يعملون لمصلحتها. ٢. كل من أذاع بأية طريقة سراً من أسرار الدفاع عن البلاد.

٣. كل من نظم أو استعمل أية وسيلة من وسائل التراسل بقصد الحصول على سر من أسرار الدفاع عن البلاد أو تسليمه أو إذاعته. وتكون العقوبة السجن إذا وقعت الجريمة في زمن الحرب."، وما ورد بالمادة (٩٠) وغيرها من مواد قانون العقوبات المصري.

أولًا- تعريف الباحث:

انطلاقًا مما سبق، يعرّف الباحث القصد الجنائي في الجانب المعنوي لجريمة اختراق المواقع الإلكترونية بأنه: تعمد الشخص تنفيذ أعمال تقنية عبر الإنترنت من شأنها الإضرار بهذه المواقع، مع إدراكه التام بأن هذه الأفعال يعاقب عليها القانون الاتحادي. ويُعد القصد الجنائي هو الجانب النفسي للجريمة أو ما يعرف بالركن المعنوي، ومن ثم لا يكفي لثبوت جريمة الاختراق أن يقوم الشخص بفعل مادي يضر بمواقع الدولة، بل يجب أن يكون هذا الفعل مقترنًا بإرادة واعية لارتكاب الجريمة. وبمعنى آخر، إذا أقدم أحد على سلوك معين يُعد مخالفًا للقوانين التي تنظم المجتمع وتحميه، فلا يكفي مجرد ارتكاب هذا السلوك لاعتباره جريمة، ما لم يكن الفاعل قد قام به بنية إحداث النتيجة المحظورة. فالجريمة ليست مجرد تصرف مادي بل تتضمن أيضًا عنصرًا نفسيًا يتمثل في الإرادة والنية، ولا يتحقق المسؤول عن الجريمة الإلكترونية إلا إذا توافرت رابطة نفسية واضحة بين الفعل الإجرامي وشخص مرتكبه، وهذه الرابطة هي أساس مساءلته قانونًا(٧٢).

ثانيًا- عناصر القصد الجنائي العام:

يرى الفقهاء أن هناك اتجاهين رئيسيين لتحديد مكونات القصد الجنائي العام:

الاتجاه الأول يقوم على أن القصد يتحقق بمجرد توافر إرادة الجاني في ارتكاب الفعل، مع علمه الكامل بما يترتب على فعله من نتائج غير مشروعة، وما يحيط به من ظروف وملابسات. ولا يشترط أن تتجه إرادته نحو تحقيق تلك النتائج، بل يكفي مجرد إدراكه لها أو توقعه إمكانية حدوثها.

أما الاتجاه الثاني، فيعرف بنظرية الإرادة، ويشترط لقيام القصد الجنائي أكثر من مجرد العلم، حيث لا يتحقق القصد إلا إذا اتجهت إرادة الجاني فعلًا نحو تحقيق النتيجة الإجرامية. ويعني ذلك ضرورة أن تكون نية الجاني متجهة بشكل صريح إلى العناصر الواقعية للجريمة، والتي تشكل الجانب المادي منها، مع وعيه الكامل بها(٧٣).

وفيما يلي نتحدث بإيجاز عن العلم والإرادة على النحو التالي:

---

(٧٢) كامل السعيد، شرح الأحكام العامة في قانون العقوبات، ط١، دار الثقافة للنشر، الأردن، ٢٠٠٢م، ص٤٦٨.

(٧٣) د. أحمد فتحي سرور، الوسيط في قانون العقوبات- القسم العام، ط٧، دار النهضة العربية، القاهرة، ٢٠١٦م، ص٥٧٢.

العنصر الأول- العلم:

يعتمد تحديد مدى توافر عنصر العلم في القصد الجنائي العام، في جريمة اختراق المواقع الإلكترونية على فهم دقيق لما يجب أن يعرفه الجاني حتى يُعدّ قاصداً ارتكاب هذه الجريمة، وذلك على مستويين:

(١) معرفة الجاني بالوقائع المتعلقة بالجريمة: يشترط أن يكون مرتكب هذه الجريمة مدركًا تمامًا للحقائق والظروف التي تندرج تحت النص القانوني المجرّم لهذا الفعل، أي أن يعلم بطبيعة الفعل الذي يقوم به، وبكونه موجهًا ضد موقع إلكتروني رسمي تابع للدولة، مما يسهم في قيام الجريمة بشروطها التي نص عليها القانون.

(٢) إدراك الجاني لركني الجريمة: ويقصد به إدراك الجاني للعناصر التي تُكوّن الجريمة من الناحية القانونية. هذا الإدراك يُفترض من حيث المبدأ، على اعتبار أن الجهل بالقانون لا يُعدّ عذراً. ولكن يظل هناك استثناء، يتمثل في الحالات التي يكون فيها الجهل أو الخطأ متعلقًا بالوقائع لا بالنص القانوني، كما لو كان الجاني لا يعلم أن استخدامه لأحد الأجهزة بوسيلة معينة يعد مخالفة قانونية. في هذه الحالة قد يُنفى عنه القصد الجنائي، لأنه لم يكن على وعي بمخالفة فعله للنظام القانوني. أما إذا كان الجهل متعلقًا بالقانون نفسه، فإن هذا لا يعفيه من المسؤولية، وفقًا للأصل العام الذي لا يجيز التذرع بعدم العلم بالقانون [٧٤].

العلم بموضوع الحق محل الحماية الجنائية:

لكي يتحقق القصد الجنائي في جريمة اختراق المواقع الإلكترونية الرسمية، لا بد أن يكون الجاني مدركًا تمامًا لطبيعة المصلحة التي يسعى القانون لحمايتها، وأن يكون على علم بأن تصرفه – سواء أكان فعلًا إيجابيًا أم امتناعًا عن القيام بما يجب – قد يؤدي إلى الإضرار بمقدرات الدولة أو يُشكل تهديداً لأمن المجتمع واستقراره. وهذا الفهم يتماشى مع ما جاء في المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١، الذي أوضح خطورة هذه الأفعال واعتبرها من الجرائم الموجهة ضد البنية الرقمية للدولة[٧٥]،وبالمثل، جاء القانون المصري رقم ١٧٥ لسنة ٢٠١٨ الخاص بمكافحة جرائم تقنية

---

(٧٤) د. محمد سلامة، جرائم الكمبيوتر والإنترنت، المكتب العربي الحديث، الإسكندرية، ٢٠٠٧م، ص١٧٤.

(٧٥) وكذلك ما ورد في المادة (٤٢) من القانون الاتحادي رقم (٥) لسنة ٢٠١٢م، بشأن مكافحة الجرائم المعلوماتية =

المعلومات ليؤكد على ضرورة أن يكون مرتكب الجريمة مدركًا لطبيعة فعله، ومدى مخالفته للقوانين التي تهدف إلى حماية أمن المعلومات والأنظمة الإلكترونية.

كما يشترط أن يكون الفاعل على دراية كاملة بالمكان الذي يُنفذ فيه جريمته، وأن يكون على علم بالنتائج التي قد تترتب على تصرفه الإجرامي المتعمد. وبناءً عليه، يجب أن يُدرك مرتكب الفعل أن ما قام به قد يترتب عليه إلحاق أذى كبير بأحد أنظمة الدولة، أو أن يؤدي إلى الإخلال باستقرار نظام الحكم، أو أن يتضمن فعلًا يُعد اعتداءً صريحًا على الدولة وفقًا لما يقره القانون الإماراتي(٢).

العنصر الثاني: الإرادة.

إن معرفة الجاني بالفعل الذي قام به لا تكفي وحدها لقيام جريمة اختراق المواقع الإلكترونية ، بل لا بد أن تكون لديه نية واضحة لتحقيق الهدف الذي دفعه لارتكاب هذا السلوك. فالقصد الجنائي لا يكتمل إلا إذا كان الفاعل قد أقدم على فعله بكامل إرادته، وكان يهدف من ورائه إلى الوصول إلى نتيجة معينة. وهذا ما يُميز الجرائم العمدية عن غير العمدية. ويتضح من ذلك أن الإرادة تتكوّن من عنصرين أساسيين: الأول هو الرغبة في القيام بالفعل الإجرامي، والثاني هو السعي إلى تحقيق النتيجة التي تترتب عليه.

(١)**إرادة النشاط:** لكي تتحقق الإرادة كجزء أساسي من القصد الجنائي، يجب أن يكون الفاعل عازمًا على تنفيذ الفعل المنسوب إليه، وأن يسعى فعليًا لتحقيقه. فإذا قام الشخص باستخدام الإنترنت في نشاط مباح، لكنه ألحق ضررًا بنظام إلكتروني تابع للدولة عن طريق الخطأ، أو نشر مادة تحرّض على تخريب المواقع الرسمية دون أن يدرك أنها مخالفة، فإن هذا يدل على غياب النية المتعمدة لارتكاب الفعل المحظور. وبالتالي، فإن مثل هذه الواقعة لا تُعد جريمة عمدية، لعدم توافر الإرادة في ارتكاب الفعل الإجرامي(٧٦).

(٢)**إرادة تحقيق النتيجة:** تُعد نية الوصول إلى النتيجة من أبرز مكونات القصد الجنائي، خصوصًا في الجرائم التي تترتب عليها نتائج ملموسة، أما في الجرائم التي يكفي فيها الفعل وحده، فإن توفر نية

الملغي.

(٢) د. محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن، ٢٠٠٩م، ص٧٨.

(٧٦) د. غنام محمد غنام، الوجيز في شرح قانون العقوبات – القسم العام، مرجع سابق، ص٢١٤.

الفاعل للقيام بالفعل غير المشروع يكون كافيًا. وتبرز أهمية هذا العنصر في التمييز بين الفعل العمدي والفعل غير العمدي، إذ قد يكون الشخص على علم تام بظروف الجريمة، ويرتكب الفعل عن قصد، لكنه لا يبتغي تحقيق النتيجة، ففي هذه الحالة نكون أمام فعل غير عمدي. فمثلًا، إذا عبث أحدهم دون قصد بنظام حاسب آلي تابع للدولة، وكان مدركًا لما يفعله، وربما توقع أن يترتب عليه فقدان للبيانات، لكنه كان يثق في قدراته ويظن أنه سيتجنب ذلك، فإننا هنا أمام خطأ غير عمدي ناتج عن الثقة الزائدة، وليس عن نية إجرامية. أما إذا كان الفاعل يريد حدوث نتيجة معينة ولم تقع، فإن المسؤولية تكون عن محاولة الجريمة، طالما أن عدم تحقق النتيجة لم يكن ناتجًا عن اختياره أو إرادته(٧٧).

ويُعبر الباحث عن رأيه بأن الوقوع في الخطأ بشأن نوع الفعل لا يُلغي توفر القصد الجنائي، فإذا كان الجاني قد تعمد القيام بأحد الأفعال المجرّمة، مثل حذف البيانات أو إرسال رسائل إلكترونية ضارة أو غيرها من الأنشطة التي يحرّمها القانون، فإن ذلك يُعد كافيًا لتحميله المسؤولية، سواء أصابت أفعاله الهدف الذي قصده بالضبط أم أخطأ فطال غيره. ففي جميع الأحوال، يُحاسب الجاني وفقًا لأحكام القانون الإماراتي على ارتكاب جريمة اختراق المواقع الرسمية للدولة. كما يشير الباحث إلى أن إثبات النية أمر معقد، لأنها ترتبط بما في داخل النفس، لكن يمكن فهمها من خلال التصرفات التي قام بها الجاني، وهي مسألة تُترك لتقدير القاضي، الذي يُقيّمها بناءً على تفاصيل الواقعة وسلوك المتهم (٧٨).

المطلب الثاني

القصد الجنائي الخاص

يتضح مما سبق أن القصد الجنائي يُعد قصدًا عامًا عندما يُقدم الجاني على ارتكاب الجريمة عن وعي وإدراك كامل بأن ما يقوم به هو فعل محظور في الأصل، ويعاقب عليه القانون. وبناءً على ذلك، فإن معظم الجرائم يتحقق فيها هذا النوع من القصد، لأن الجاني يُنفذ السلوك الإجرامي وهو مدرك لطبيعته غير المشروعة، كأن يقوم مثلًا بنشر معلومات تتضمن تحريضًا على ارتكاب جرائم

---

(٧٧) المرجع السابق، ص٢١٥.

(٧٨) د. أحمد شوقي عمر أبو خطوة، شرح الأحكام العامة لقانون العقوبات، مرجع سابق، ص٢٨٦.

تتعلق باختراق المواقع الإلكترونية الرسمية التابعة للدولة[٧٩].

أما القصد الجنائي الخاص، فهو أعمق من القصد العام، بل يمكن اعتباره مكمّلًا لـه أو مكوّنًا أساسيًا منه في بعض الحالات. ففي بعض الجرائم، يشترط المشرّع أن تكون لدى الجاني نية محددة أو هدف خاص يسعى إلى تحقيقه، كإحداث ضرر معين أو الوصول إلى نتيجة بعينها. وعند توافر هذا العنصر، نكون أمام قصد جنائي خاص. وهذا ما ينطبق على جريمة اختراق المواقع الإلكترونية ، حيث لا يكفي مجرد تنفيذ الفعل، بل يجب أن يكون الجاني قد قصد عمدًا الإخلال بأنظمة الإدارة أو التلاعب بأرصدة البنوك[٨٠].

وبناءً على ذلك، يمكن القول إن القصد الخاص هو توجه إرادة الجاني نحو تحقيق هدف معين من وراء ارتكاب الجريمة. وفي الأصل، لا يُعتد بالدافع الذي حرّك الجاني لارتكاب الفعل أو بتوافر القصد الجنائي العام، فالدافع في حد ذاته – باعتباره الغاية التي يسعى الجاني إلى بلوغها – لا يُعد عنصراً من عناصر الركن المعنوي للجريمة. غير أن المشرّع الإماراتي قد يعتد في بعض الحالات بهذا الدافع، ويُدخله ضمن عناصر القصد الجنائي. وهنا لا يكون الحديث عن مجرد باعث عادي، بل عن قصد خاص يتمثل في نية الجاني لتحقيق واقعة قد تكون منفصلة عن عناصر الجريمة المادية والمعنوية. ويُطلق على هذا النوع من الدوافع "القصد الجنائي الخاص" لتمييزه عن الدوافع التي لا يعتد بها القانون. وعندما يشترط القانون هذا القصد الخاص، فإن غيابه يؤدي إلى سقوط الجريمة، ما لم يُقرر القانون وصفًا تجريمياً آخر للفعل محل الواقعة[٨١].

في بعض الجرائم الإلكترونية، ومنها الجريمة محل البحث، لا يُكتفى بوجود القصد الجنائي العام، بل يُشترط أيضًا توفر قصد خاص حتى تُعد الجريمة قائمة. أي أن الجاني لا يُساءل لمجرد قيامه بفعل التسلل أو التلاعب بالأنظمة، بل يجب أن تكون نيته واضحة ومتجهة نحو استهداف المواقع الرسمية للدولة، إما بهدف الإضرار بها أو الدخول إليها دون تصريح. وهذا ما يميز هذه الجريمة عن

---

(٧٩) د. أحمد أبو الروس، القصد الجنائي والمساهمة والمسئولية الجنائية والشروع والدفاع الشرعي وعلاقة السببية، ط٢، المكتب الجامعي الحديث، الإسكندرية، ٢٠١١م، ص٤٠.

(٨٠) د. عبد الفتاح مصطفى الصيفي، قانون العقوبات النظرية العامة، دار الهدى للمطبوعات، القاهرة، ٢٠٠٣م، ص٣١١.

(81) Cyber warfare and Cyber terrorism. Lech Jaycee Wish, Idea Group Inc. 2008, P. 112.

غيرها من الجرائم الإلكترونية ذات الطابع العام، إذ يُشترط في هذه الحالة أن تكون الإرادة موجهة لتحقيق غاية محددة ترتبط بالمصلحة التي يحميها القانون(٨٢).

وحين يشترط المشرع وجود قصد خاص، قد يحدث خلط بين هذا القصد وبين الباعث الذي دفع الجاني لارتكاب الجريمة، إلا أن هذا الخلط لا يؤثر على تكييف الجريمة أو تقدير عقوبتها. ففي الحالات التي يتداخل فيها القصد مع الباعث، لا يُعتد بالباعث باعتباره مجرد دافع نفسي أو شخصي، بل يُنظر إليه على أنه جزء من القصد الجنائي الخاص، أي أنه عنصر لازم لتحقق الجريمة، وليس مجرد سبب دفع الجاني لارتكابها(٨٣).

عندما يشترط القانون الإماراتي توفر قصد جنائي خاص في جريمة اختراق المواقع الإلكترونية فإن هذا القصد يُضاف إلى القصد العام، ولا يُعد بديلاً عنه. بمعنى أن الجاني يجب أن يكون قد ارتكب الفعل بإرادة حرة ووعي تام (وهو القصد العام)، إضافة إلى وجود نية محددة تستهدف تحقيق غرض معين من ذلك الفعل (وهو القصد الخاص). ولهذا السبب، تُصنف هذه الجرائم ضمن الجرائم العمدية فقط، لأنه لا يمكن تصور تحقق القصد الجنائي الخاص في الأفعال التي ترتكب بسبب الإهمال أو الخطأ، أي في الجرائم غير العمدية (٨٤).

من أبرز الفروقات بين القصد الجنائي العام والقصد الجنائي الخاص، أن نية الجاني في القصد الخاص تتجه نحو تحقيق غاية إضافية لا تُعد من المكونات الأساسية للجريمة، في حين أن القصد العام يقتصر على نية ارتكاب الفعل والنتيجة التي تُشكّل الجريمة ذاتها. فمثلًا، إذا أقدم شخص على الدخول إلى شبكة الإنترنت بهدف التخريب، فإن فعل الدخول يُمثل العنصر المادي للجريمة، أما الغاية التي يسعى لتحقيقها من هذا الفعل، كإحداث خلل أو تعطيل في نظام معين، فهي تمثل القصد الجنائي الخاص الذي يتجاوز الفعل المادي ويُكمل الصورة الكاملة للجريمة (٨٥).

---

(٨٢) د. أحمد شوقي عمر أبو خطوة، شرح الأحكام العامة لقانون العقوبات، مرجع سابق، ص٣١٦.

(٨٣) ماهر عبده شويش الدرة، الأحكام العامة في قانون العقوبات، وزارة التعليم العالي والبحث العلمي بجامعة الموصل- العراق، ١٤١٠هـ، ص٣١٣.

(٨٤) د. غنام محمد غنام، الوجيز في شرح قانون العقوبات- القسم العام، مرجع سابق، ص٢٢٢.

(٨٥) د. محمود نجيب حسني، شرح قانون العقوبات- القسم العام، مرجع سابق، ص ٦٢٨.

يتضح من ذلك أن القصد الجنائي الخاص يقوم في الأساس على نفس عناصر القصد العام، وهما: إرادة الجاني في ارتكاب الفعل، وعلمه بطبيعته غير المشروعة، ثم يُضاف إلى هذين العنصرين عنصر ثالث، يتمثل في الغاية أو الدافع الذي يسعى الجاني إلى تحقيقه، بشرط أن يكون هذا الدافع أو الغاية قد نص عليها القانون بشكل صريح كجزء من القصد الواجب توافره للجريمة(٨٦).

(٨٦) د. أحمد فتحي سرور، الوسيط في قانون العقوبات- القسم العام، مرجع سابق، ص٣٥٠.

الخاتمـة

أولًا – نتائج الدراسة:

١. إدراك المشرّع وتطور التشريع: يُبيّن تطور القوانين في كل من الإمارات ومصر وجود وعي قانوني متقدم تجاه الجرائم الإلكترونية الحديثة، وخصوصاً ما يتعلق باختراق المواقع الرسمية. فقد حرص المشرعان على عدم الاكتفاء بالنصوص القديمة، بل بادرا إلى تعديلها وتطويرها بما يتوافق مع التغيرات السريعة في المجال الرقمي. وعلى الرغم من وجود بعض أوجه القصور، إلا أن الخطوات التي تم اتخاذها تُعد من أبرز المحاولات العربية في مواجهة هذه الظواهر المتجددة.

٢. طبيعة الجريمة وتصنيفها: تُعد جريمة اختراق المواقع الرسمية من الجرائم الرقمية المتقدمة التي تتسم بطابعها العابر للحدود، حيث يمكن تنفيذها من أي مكان حول العالم، ما دام مرتكبها يملك القدرة الفنية اللازمة، دون أن يكون هناك ارتباط بمكان أو زمان محدد.

٣. المسؤولية الجنائية لمستخدمي الإنترنت: يُحاسب مستخدم الإنترنت جنائيًا إذا قام بارتكاب فعل مجرّم من خلال الشبكة، وتظل هذه المسؤولية قائمة ما لم يتم إثبات عكسها، كأن يكون الجهاز قد استُخدم من طرف آخر دون علم أو موافقة من المستخدم الأصلي.

٤. مكونات الجريمة: لا تتحقق المسؤولية الجنائية في الجريمة موضع الدراسة إلا بتوافر عنصرين رئيسيين، هما: الفعل المادي الذي يُجسد الاعتداء، والقصد الجنائي الذي يكشف عن نية الجاني، ولا يمكن اعتبار الجريمة قائمة دون تحقق هذين العنصرين معًا.

٥. أنماط السلوك الإجرامي: تتنوع الأفعال التي تُشكل هذه الجريمة، ويُعد الدخول غير المصرح به إلى الأنظمة الإلكترونية أبرز تلك الأفعال، سواء كان الهدف هو الإفساد، أم الاطلاع غير المشروع، أو التعديل على البيانات والمحتوى.

٦. صعوبة تحديد الجناة: تبرز صعوبات فنية حقيقية في تتبع هوية مرتكبي هذا النوع من الجرائم، خاصة عندما يستخدم الجاني أجهزة عامة أو أدوات لإخفاء هويته الرقمية، ما يعقد مهمة جهات التحقيق.

٧. إخفاء الهوية الرقمية:يستخدم الجناة وسائل تقنية متعددة لطمس آثارهم، كاستخدام شبكات VPN، أو الأجهزة العامة (كمراكز الإنترنت أو مطارات)، مما يصعب تتبعهم جنائيًا.

٨. عقبات في الملاحقة الدولية: تواجه السلطات القانونية صعوبات كبيرة في ملاحقة الجناة دولياً، خاصة إذا تم ارتكاب الجريمة من خارج حدود الدولة، مما يثير إشكاليات تتعلق بالاختصاص القضائي والتعاون الدولي.

٩. قابلية الشبكات للاختراق: من أبرز أسباب تفشي هذه الجريمة سهولة اختراق البنية التحتية الرقمية، نتيجة ضعف الحماية الإلكترونية، وغياب الرقابة الكافية على المنصات الاجتماعية والمعلوماتية.

١٠. التميّز عن الجرائم الإلكترونية الأخرى: تتمتع هذه الجريمة بخصائص فنية وقانونية تجعلها متميزة عن غيرها من الجرائم الإلكترونية، لا سيما من حيث هدفها، وخطورتها على الأمن القومي، ومرتكبيها ذوي الكفاءة التقنية العالية.

ثانيًا- توصيات البحث:

١. استناداً إلى ما توصلت إليه الدراسة من نتائج، يوصي الباحث بالآتي:

٢. تعزيز التعاون الدولي: تبرز أهمية العمل المشترك بين الدول لتوحيد الجهود في مواجهة جريمة اختراق المواقع الإلكترونية الرسمية، من خلال وضع إطار قانوني دولي موحد يحدد بشكل دقيق آليات التفتيش والضبط والتحقيق في هذه النوعية من الجرائم. ويُفترض أن يتضمن هذا الإطار وسائل فعّالة لتسهيل التعاون القضائي بين الدول، بما يمكّن من تعقّب الجناة وتقديمهم للعدالة، بغض النظر عن أماكن وجودهم أو جنسياتهم.

٣. تشكيل لجان ثنائية بين الإمارات ومصر: ضرورة إنشاء لجان مشتركة دائمة بين مصر والإمارات لمواجهة هذه الجريمة بصفة وقائية وتشريعية وتقنية، خاصة في ظل ريادة البلدين إقليمياً في مجال البنية التحتية التكنولوجية، مما يجعلهما من الأهداف الرئيسية للهجمات الإلكترونية.

٤. رفع كفاءة موظفي الدولة في المجال المعلوماتي: التأكيد على أهمية نشر الوعي الأمني المعلوماتي بين موظفي الجهات الحكومية، خاصة أولئك الذين يتعاملون مع البيانات الحساسة، مع إلزامهم بتلقي تدريبات دورية حول سبل تأمين البيانات وحماية الأنظمة الإلكترونية من الاختراق.

٥. مواصلة تطوير التشريع الإماراتي: نهيب بالمشرّع الإماراتي، الذي كان سبّاقًا في مواجهة

الجرائم الإلكترونية، الاستمرار في تطوير تشريعاته بما يتلاءم مع التطور المتسارع لطبيعة هذه الجريمة، ليبقى في مقدمة التشريعات العالمية والعربية.

٦. تحصين البنية المعلوماتية: ضرورة تحصين البنية التحتية الرقمية والاجتماعية ضد الاختراق، من خلال تحديث الأنظمة الدفاعية الرقمية، ووضع سياسات واضحة للحد من ثغرات الأمن السيبراني، وضمان بيئة تصفح آمنة للمستخدمين.

٧. اعتبار الجريمة ذات طابع دولي: التأكيد على أن جريمة اختراق المواقع الإلكترونية الرسمية جريمة ذات طابع دولي، نظراً لآثارها العابرة للحدود، وضرورة تبني موقف دولي موحد يجرّمها صراحة، ويضع إطاراً قانونياً للتعاون في مكافحتها.

٨. معالجة الأسباب الاجتماعية لانتشار الجريمة: وجوب القضاء على العوامل الاجتماعية والاقتصادية التي تسهم في تفشي الجرائم الإلكترونية، مثل البطالة، وضعف الوعي الثقافي والأمني، وضرورة تعزيز التوازن السياسي والاقتصادي داخل الدولة.

٩. تعزيز التدابير الفنية لحماية الأنظمة: التأكيد على ضرورة اتخاذ الإجراءات الفنية المناسبة لتأمين المواقع الإلكترونية الحساسة، وتعزيز نظم الحماية الإلكترونية في المؤسسات الرسمية، لتكون قادرة على التصدي لمحاولات الاختراق بشكل فوري وفعّال.

قائمة المراجع

أولًا- المراجع العامة:

(١) د. أحمد أبو الروس، القصد الجنائي والمساهمة والمسئولية الجنائية والشروع والدفاع الشرعي وعلاقة السببية، ط٢، المكتب الجامعي الحديث، الإسكندرية – مصر، ٢٠١١م.

(٢) د. أحمد شوقي عمر أبو خطوة، شرح الأحكام العامة لقانون العقوبات، دار النهضة العربية، القاهرة، ٢٠٠٠م.

(٣) د. أحمد فتحي سرور: الوسيط في قانون العقوبات- القسم العام، ط٧، دار النهضة العربية، القاهرة، ٢٠١٦م.

(٤) د. أحمد عوض بلال، مبادئ قانون العقوبات المصري "القسم العام"، دار النهضة، القاهرة، بدون سنة نشر.

(٥) د. أحمد المجدوب، التحريض على الجريمة، دراسة مقارنة، بدون رقم طبعة، الهيئة العامة لشئون المطابع الأميرية، القاهرة – مصر، ١٩٨٧م.

(٦) د. حسن محمد ربيع، شرح قانون العقوبات الاتحادي، ط١، أكاديمية شرطة دبي، الإمارات العربية المتحدة، ٢٠٠٦م.

(٧) د. طلعت الشهاوي، المسئولية الجنائية عن جرائم الاتصالات – دراسة مقارنة مع قوانين الاتصالات في فرنسا والولايات المتحدة الأمريكية والمملكة العربية السعودية والإمارات وفطر وليبيا وتونس ولبنان والكويت وسلطنة عمان والسودان وسوريا والأردن وفلسطين والبحرين، دار النهضة العربية، القاهرة، ٢٠١٩م.

(٨) د. عبد الفتاح مصطفى الصيفي، قانون العقوبات النظرية العامة، دار الهدى للمطبوعات، القاهرة، ٢٠٠٣م.

(٩) د. عبود السراج، قانون العقوبات – القسم العام، بدون رقم طبعة، منشورات جامعة حلب، سوريا، ١٩٩٧م.

(١٠) د. غنام محمد غنام: الوجيز في شرح قانون العقوبات – القسم العام، ط١، مطبعة جامعة المنصورة الجديدة، المنصورة، ٢٠٠٨م.

(١١) كامل السعيد، شرح الأحكام العامة في قانون العقوبات، ط١، دار الثقافة للنشر، الأردن،

٢٠٠٢م.

(١٢) ماهر عبده شويش الدرة: الأحكام العامة في قانون العقوبات، وزارة التعليم العالي والبحث العلمي بجامعة الموصل- العراق، ١٤١٠هـ.

(١٣) د. مأمون محمد سلامة: قانون العقوبات القسم العام، مطبعة جامعة القاهرة والكتاب الجامعي، القاهرة – مصر، ١٩٩٦م.

(١٤) د. محمد الحديثي، جرائم التحريض وصورها في الجوانب الماسة بأمن الدولة الخارجي وفقًا للتشريع العراقي، مطابع وزارة الثقافة والإعلام، بغداد – العراق، ١٩٨٤م.

(١٥) د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها علي قانون العقوبات، دار النهضة العربية، القاهرة، ٢٠٠٣م.

(١٦) د. محمد الشهاوي، شرح قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣، ط١، دار النهضة العربية، القاهرة، ٢٠١٠م.

(١٧) د. محمد عبد اللطيف عبد العال: النظرية العامة للجريمة والمسؤولية الجنائية في القانون الكويتي، مجلس النشر العلمي، جامعة الكويت، ٢٠١٥م.

(١٨) د. محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٩م.

(١٩) د. محمود نجيب حسني، شرح قانون العقوبات- القسم العام، ط٨، دار النهضة العربية، القاهرة – مصر، ٢٠١٦م.

(٢٠) د. محمود نجيب حسني، علاقة السببية في قانون العقوبات، طبعة نادي القضاة، القاهرة – مصر، ١٩٨٤م.

(٢١) د. معن أحمد الحياري، الركن المادي للجريمة، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠١٠م.

ثانيًا: المراجع المتخصصة:

(١) إبراهيم عبد الخالق، الشامل في جرائم الإنترنت في ضوء قانون العقوبات، المكتب الفني للإصدارات القانونية، القاهرة، ٢٠٢١م.

(٢) د. جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي- الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ٢٠١٢م.

(٣) حسين بن سعيد الغافري، السياسة الجنائية في مواجهة الإنترنت – دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٩م.

(٤) د. سوزي عدلي ناشد: الإرهاب الإلكتروني بين الاقتصاد الخفي والاقتصاد الرسمي، ط١، دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠٥م.

(٥) د. عادل عبدالصادق، الفضاء الإلكتروني والعلاقات الدولية– دراسة في النظرية والتطبيق، ط١، المكتبة الأكاديمية، القاهرة، ٢٠١٦م.

(٦) د. محمد سلامة: جرائم الكمبيوتر والإنترنت، المكتب العربي الحديث، الإسكندرية – مصر، ٢٠٠٧م.

(٧) محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والإنترنت، منشأة المعارف، الإسكندرية، ٢٠٠٦م.

(٨) د. مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٠م.

(٩) نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، ٢٠٠٨م.

(١٠) د. هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقاً عليها، ط٢، دار النهضة العربية، ٢٠١١م.

(١١) د. ياسر نوار، المواجهة التشريعية والأمنية لجرائم التجارة الإلكترونية، ط١، بدون دار نشر، ٢٠١٢م.

ثالثًا: الرسائل الجامعية:

(١) حسن بن محمد السلطان، تجريم تمويل الإرهاب والعقاب عليه– دراسة تحليلية مقارنة، رسالة ماجستير، جامعة نايف للعلوم الأمنية، الرياض – المملكة العربية السعودية، ٢٠٠٩م.

(٢) خالد بن محمد سليمان المرزوق، جريمة الإتجار بالنساء والأطفال وعقوباتها في الشريعة الإسلامية والقانون الدولي – دراسة تأصيلية مقارنة، رسالة ماجستير، جامعة نايف للعلوم الأمنية، الرياض – المملكة العربية السعودية، ٢٠٠٥م.

(٣)د. علي محمود علي حموده، النظرية العامة في تسبيب الحكم الجنائي في مراحله المختلفة

"دراسة مقارنة، رسالة دكتوراه، القاهرة، ١٩٩٤م.

(٤) ماجد بن كريم الزارع، الركن المادي في الجرائم الإكترونية في النظام السعودي – دراسة تأصيلية، رسالة ماجستير، جامعة نايف للعلوم الأمنية، الرياض – المملكة العربية السعودية، ٢٠١٤م.

رابعًا: الأبحاث العلمية:

(١) دلال لطيف مطشر، على المواقع الإلكترونية– دراسة مقارنة، مجلة جامعة بابل للعلوم الإنسانية، المجلد ٢٦، العدد ٩، ٢٠١٨م.

(٢) صباح كزيز، د. سمير قط، أثر الجرائم الإلكترونية على أمن واستقرار الدول: قرصنة الموقع الإلكتروني لوكالة الأنباء القطرية أنموذجًا، مخبر أثر الاجتهاد القضائي على حركة التشريع – كلية الحقوق والعلوم السياسية، جامعة محمد خيضر – بسكرة، الجزائر، مجلة الناقد للدراسات السياسية، العدد الثالث، أكتوبر ٢٠١٨م.

(٣) عمر حوتية، وآخرون، تجربة دولة الإمارات في التصدي للجرائم المعلوماتية الواقعة على التجارة الإلكترونية) المجلة الأردنية للمكتبات والمعلومات – جمعية المكتبات والمعلومات الأردنية– الأردن، المجلد ٥٠ العدد ٤، كانون الأول ٢٠١٥م.

(٤) د. محمد قيراط، الإعلام الجديد والإرهاب الإلكتروني: آليات الاستخدام وتحديات المواجهة، مجلة الحكمة للدراسات الإعلامية والاتصالية – مؤسسة كنوز الحكمة للنشر والتوزيع – الجزائر، العدد التاسع، يناير ٢٠١٧م.

خامسًا: الندوات العلمية:

(١) د. رفعت رشوان، سياسة المشرع الإماراتي الجنائية في مواجهة الجرائم البيئية، ندوة علمية حول مكافحة جرائم البيئة، القيادة العامة لشرطة أبو ظبي، مركز البحوث والدراسات الأمنية..

سادسًا: المعاجم اللغوية:

(١) د. جرجس جرجس: معجم المصطلحات الفقهية والقانونية، مراجعة: القاضي انطوان الناشف، ط١، الشركة العالمية للكتاب، بيروت، ١٩٩٦م.

سابعًا: المراجع الأجنبية:

(1) Ibrahim El-Shahat Lotfy,"The crime of electronic hacking in UAE

legislation", International Journal of Advanced Research on Law and Governance, Volume 5, Issue 2, 2023.

(2) First annual cost of cybercrime study, penman institute, research report mi.2010, cyber warfare and cyber terrorism. Lech Jaycee wish, idea group inc. 2008