جامعة المنصورة
كلية الحقوق
إدارة الدراسات العليا
قسم القانون الجنائي

أحكام التجريم لجرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة

إشراف

الأستاذ الدكتور/ تامر محمد محمد صالح
أستاذ القانون الجنائي
وكيل كلية الحقوق جامعة المنصورة

إعداد الباحث

عبد الله بن سالم بن سعيد الكعبي

باحث دكتوراه بقسم القانون الجنائي
كلية الحقوق جامعة المنصورة

٢٠٢٣م

المقدمة

أولًا: موضوع الدراسة:

لقد أصبحت المعلومة هي السلعة الرئيسية في العالم كله، حيث إن الدول لن تقاس بجيوشها أو قواتها أو ثروتها في الوقت الحالي، ولكن المقياس الأول لقوة الدولة هي مقدار ما تنتجه من معلومات ومن صناعة المعلومات واستخدامها والتعامل معًا، فالمعلومة قوة هذا الانفجار المعلوماتي حيث أصبح الاعتداء على سلامة الشبكات والأنظمة والتقنيات المعلوماتية – الخاصة بالدولة– إلى حد كبير سواء من دخول غير مشروع على تكنولوجيا الاتصالات وتكنولوجيا الحاسب الآلي الخاص بالدولة، وسواء من حيث تعطيل وإعاقة البيانات والاعتداء على سلامتها والدخول غير المشروع إليها(١).

ولقد زادت جرائم الاختراق والاعتداء على المعلومات والبيانات الخاصة بمؤسسات الدولة، وكذلك جرائم تدمير ونقل البيانات والمعلومات المرفوعة على شبكة الإنترنت أو غيرها من الشبكات من خلال المواقع الإلكترونية أو الأنظمة المعلوماتية الخاصة بالدولة، مما يعد تطوراً في الأساليب الجرمية باستخدام التكنولوجيا، نظراً لاختراق المجرمين هذه المعلومات والبرامج، والولوج إليها، والاعتداء على محتواها بتغييرها، أو إتلافها، أو سرقتها، مما دفع المشرع الجزائي في الكثير من دول العالم إلى تجريم هذه الأفعال والمعاقبة عليها.

وتعد جرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة إحدى أنواع الجرائم المعلوماتية التي تهاجم المواقع الرسمية للحكومات، وأنظمة شبكاتها، وتركز على تدمير البنى التحتية لهذه المواقع، أو الأنظمة الشبكية الخاصة بالدولة بشكل كامل، والتي قد تتنوع بدورها إلى ما يُعرف بالتجسس الإلكتروني، والتدمير والإتلاف الإلكتروني، وكذلك الدخول أو البقاء غير المشروع داخل النظام المعلوماتي، ولقد زاد من أهمية التصدي لهذه الجرائم ارتباطها في بعض الأحيان مع الأمن المعلوماتي الوطني، وهو على جانب كبير من الأهمية لكثير من الدول، فبعض الأنظمة المعلوماتية الخاصة بالدولة قد تحتوي على أسرار غاية في الأهمية للدولة، وذات تأثير على الأمن والاقتصاد الوطني، وقد يؤدي إفشاؤها إلى تهديد سلامة الدولة أو تسبب أضراراً لمصالحها أو تكون ذات فائدة لأي دولة أو جهة أخرى، كما أن العبث في أنظمة المعلومات لبعض الحسابات البنكية قد يؤدي إلى الإخلال بالمراكز القانونية لبعض العملاء سواء بتحسين المركز القانوني والمالي أو تراجعه.

ويُضاف إلى ذلك أن الشبكة المعلوماتية تحتوي على كثير من المواقع والأنظمة الإلكترونية التي تحتوي على معلومات مهمة؛ كالمواقع العسكرية، أو أنظمة التسليح، أو غيرها من المعلومات التي

---

(١) د. نور سليمان يوسف يعقوب البالول، الأحكام الموضوعية لجرائم المعلوماتية: دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ١٤٤٢هـ/٢٠٢١م، ص٤٩.

لا يجوز الاطلاع عليها إلا لمن يخوله القانون ذلك، كما أن النظام المعلوماتي الخاص بالدولة يحتوي على معلومات تمس الأمن الوطني، وبالتالي لا يجوز الدخول إليه بدون تصريح، ومن ثم؛ لا يجوز التعدي عليه أو سرقة محتواه أو نقله، فالمعلومات الموجودة بالأنظمة المعلوماتية الخاصة بالدولة تكون على شكل محتوى إلكتروني، غير أن المخزن الإلكتروني الموجود فيه تلك الأسرار تكون عرضة للاختراق، أو الحصول على هذه الأسرار وإفشائها، الأمر الذي يتعين معه تجريم كافة صور الاعتداء على هذه الأنظمة حتى لو كان هذا المحتوى محاط بوسائل الأمن المعلوماتي، حتى لا يؤدي ذلك الاعتداء لتعريض مصالح الدولة وأمنها ونظامها المعلوماتي للخطر لا سيما وأن تلك المعلومات قد تكون عسكرية أو سياسية أو اقتصادية، أو أمنية.

ونظرًا لخطورة الجرائم محل البحث المتمثلة في قيام الجاني بالدخول أو البقاء غير المشروع في النظام المعلوماتي الخاص بالدولة، أو الدخول إلى الشبكة المعلوماتية، أو نظام المعلومات أو المواقع الإلكترونية الخاصة بالدولة وذلك للحصول على محتوى إلكتروني غير متاح للجمهور، يمس الأمن الوطني أو العلاقات الخارجية للدولة أو السلامة العامة أو الاقتصاد الوطني، ومن أجل الوقوف على أحكام التجريم لجرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة؛ فإن الأمر يقتضي بيان أنماط وصور تلك الجرائم، كما يتعين الأمر بيان أركان تلك الجرائم، وهذا ما نوضحه من خلال هذا البحث.

ثانيًا: أهمية البحث:

تُعد الدوافع السياسية من أبرز المحاولات الدولية لاختراق الشبكات الحكومية في مختلف دول العالم، كما أنه قد يتمكن من اختراق الأجهزة الأمنية الحكومية، وكذلك أصبحت شبكة المعلومات مجالًا خصبًا لنشر أفكار العديد من الأفراد والمجموعات الإرهابية، ووسيلة لترويج أخبار وأمور أخرى قد تحمل في طياتها مساسًا بأمن الدولة، أو بنظام الحكم أو قدحًا في رموز دولية أو سياسية [٢]، والإساءة لها بالذم والتشهير[٣]. كما تزداد أهمية هذا البحث إذا ما سلمنا بأنه تمتلك أي دولة في العالم بعض الأسرار التي لا ينبغي لأي شخص أن يقوم بالاطلاع عليها دون إذن أو مسوغ، وأي اطلاع عليها أو اعتداء، قد يؤدي لحدوث أزمات داخلية وخارجية، حيث إن هذا النوع من المعلومات ينم عن خطورة كبيرة، لذلك فقد عمل المشرع على حماية البيانات والمعلومات، التي تؤثر على أمن الدولة الداخلي والخارجي، والمحفوظة في النظام المعلوماتي والشبكات والمواقع الإلكترونية الخاصة بها.

---

(٢) د. أشرف محمد نجيب السعيد الدريني، جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات: دراسة تحليلية مقارنة، بحث منشور في مجلة روح القوانين، كلية الحقوق، جامعة طنطا، المجلد ٩٥، العدد ٩٥، يوليو ٢٠٢١م، ص٢٩٩، ٣٠٠.

(٣) تركي بن عبد الرحمن المويشير، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، إصدارات جامعة نايف العربية للعلوم الأمنية مركز البحوث والدراسات، مركز الدراسات والبحوث، الرياض، السعودية، ٢٠١٢م، ص٣٩.

وبالإضافة إلى ما سبق تُشكل الجرائم الواقعة على النظم المعلوماتية الخاصة بالدولة في الوقت الراهن إحدى أبرز الجرائم المرتكبة، بالنظر إلى ذيوع استخدام الحواسب الآلية والتطبيقات الإلكترونية وشبكة المعلوماتية الدولية" الإنترنت" والتقنيات المستحدثة، ودخولها في كافة مناحي الحياة، بالشكل الذي بات يشكل عالمًا افتراضيًا موازيًا للعالم الواقعي، وهو ما جعل هذه التقنيات والتطبيقات مجالًا خصبًا ونطاقًا واسعًا لارتكاب العديد من الجرائم التي تمس حقوق الإنسان ومملكاته وخصوصياته؛ وهو ما يتطلب ضرورة بسط حكم القانون على هذه الأنشطة التقنية المستحدثة، وتوفير حماية قانونية متكاملة لمواجهة هذه النوعية المستحدثة من الجرائم. كما يرجع أسباب اختيار هذا البحث كذلك إلى قلة الدراسات والأبحاث السابقة التي تناولت موضوع الجرائم الواقعة على أمن الدولة المعلوماتي بشكل مستقل.

ثالثًا: إشكالية البحث:

تثير الظواهر الإجرامية المستحدثة بعض الإشكاليات القانونية المتعلقة بالقانون الجنائي الموضوعي بحثًا عن إمكانية تطبيق النصوص التقليدية على هذا النوع من الجرائم احترامًا لمبدأ الشرعية، والتفسير الضيق للنصوص الجنائية، وبالتالي يثور التساؤل حول كيفية المواءمة بين القواعد التقليدية القانونية المتعلقة بالشق الأخير وبين آلية مواجهة هذا النوع من الجرائم. كما تثير هذه الدراسة عدة إشكاليات مهمة لعل أهمها يكمن في حداثة هذه الجرائم نظرًا لارتباطها بالتقدم التكنولوجي، الأمر الذي يترتب عليه ضرورة بيان الأحكام التجريمية للجرائم الواقعة على أمن الدولة المعلوماتي، وإلى مدى نجحت النصوص الحالية عن توفير إطار تشريعي حاكم لمواجهتها.

رابعًا: منهج البحث:

سوف نعتمد في هذه الدراسة على المنهج الوصفي التحليلي. كما سيتم الاستعانة بالمنهج القانوني المقارن، وذلك بالتركيز على النصوص الجزائية في التشريعين المصري والعماني الخاصة بتجريم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة، بالإضافة إلى التشريع الكويتي والإماراتي والسعودي.

خامسًا: خطة البحث:

المبحث الأول: أنماط جرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة.

المبحث الثاني: أركان جرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة.

المبحث الأول

أنماط جرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة

تمهيد وتقسيم:

لقد تطورت الظاهرة الإجرامية في العصر الحديث تطوراً ملحوظًا ومذهلًا سواء في أشخاص مرتكبيها أو في أسلوب ارتكابها والذي يتمثل في استخدام آخر ما توصلت إليه العلوم التقنية والتكنولوجية وتطويعها في خدمة الجريمة(٤)؛ الأمر الذي أفرد نوعية جديدة سميت بجرائم التقنية، أو جرائم المعلوماتية التي ارتبطت ارتباطًا وثيقًا بشبكة المعلومات الدولية(٥).

وما تجب الإشارة إليه أنه تأخذ جرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة عدة صور، الأمر الذي يقتضي التعرض للأحكام التجريمية لهذه الصور في التشريعين المصري والعُماني والتشريعات المقارنة، وكذلك بيان الجوانب المحمية في تلك الجرائم، وذلك من خلال تقسيم هذا المبحث إلى مطلبين، وذلك على التقسيم التالي:

المطلب الأول: جرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة في التشريع المصري والمقارن.

المطلب الثاني: العلة من تجريم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة.

---

(٤) د. عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، بحث منشور في مجلة دراسات الكوفة، العراق، المجلد الأول، الإصدار السابع، السنة ٢٠٠٨م، ص١١١.

(5) Melanie Kowalski,"Cybercriminalité : enjeux, sources de données et faisabilité de recueillir des données auprès de la police", Centre canadien de la statistique juridique,No 85-558-XIF au catalogue,Décembre 2002,Consulté le 05/11/2021 à 13h15, https://www150.statcan.gc.ca/n1/fr/pub/85-558-x/85-558-x2002001-fra.pdf?st=IXUiSy_b

المطلب الأول

جرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة في التشريع المصري والمقارن

تمهيد وتقسيم:

باستقراء النصوص التشريعية لقوانين مكافحة تقنية المعلومات في القانون المصري والقوانين المقارنة يتضح جليًا أنه لم تتناول تلك التشريعات النص صراحة على جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة، على غرار التشريع المصري الذي تناولها بالتجريم في نص مستقل في قانون مكافحة جرائم تقنية المعلومات [٦]. فقد اتجه التشريع العُماني والتشريعات المقارنة إلى النص على تجريم فعل الدخول غير المشروع، وما يترتب عليه من تعديات بشكل عام دون التطرق إلى كون هذه الاعتداءات أو الانتهاكات تنصب على نظام معلوماتي خاص بالأشخاص أم بنظام حكومي خاص بالدولة. كما اكتفى البعض منها بالإشارة إلى مجرد تشديد العقوبة إذا ما كان الاعتداء قد وقع على نظام حكومي أو بيانات ومعلومات حكومية، وبالتالي يتعين بيان هذه الجريمة في القانون المصري في فرع مستقل، وبيان صور وأنماط تلك الجرائم في فرع آخر، وذلك من خلال التقسيم التالي:

الفرع الأول

جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة في التشريع المصري

تجدر الإشارة إلى أن النظام المعلوماتي للدولة لا يُعتبر أماكن خاصة أو مساكن حتى تتمتع بالحماية الجنائية المقررة لهذه الأماكن في حال دخولها دون وجه حق، كما أن الوصول إلى البيانات والمعلومات فعل خطير كون هذه البيانات والمعلومات ضعيفة داخل النظام؛ بحيث يمكن الاعتداء عليها بسهولة، مما دعا التشريعات إلى توفير حماية جنائية للنظام المعلوماتي من الولوج غير المشروع[٧]. فمثلًا نجد أن الدخول غير المصرح به للأنظمة المعلوماتية للدولة يهدد – بلا شك–العديد من المصالح المحمية، حكومية وفردية وتجارية؛ حيث إن أغلب أنظمة الحواسيب تمتلكها الحكومة، والعديد من الحكومات تعتمد في إدارتها لمرافقها على نظام الحكومة الإلكترونية، ويهدد الدخول غير المصرح به

---

(٦) فقد نص المشرع المصري عليها في نص المادة ٢٠ من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨م.

(٧) د. شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، ٢٠٠٥م، ص١٠٧–١٠٨.

لبعض الأنظمة المعلوماتية أمن الدولة الوطني، كالاطلاع على معلومات تمس أمن الدولة، أو الوصول إلى أنظمة التحكم أحياناً في محطات المفاعلات النووية[٨].

وينصرف معنى الدخول غير المشروع إلى النظام المعلوماتي لكي يشمل كافة الأفعال التي تسمح بالدخول إلى نظام معلوماتي والإحاطة أو السيطرة على المعطيات التي يتكون منها، أو الخدمات التي يقدمها، فمجرد الدخول إلى النظام المعلوماتي لا يمثل فعلًا غير مشروع في حد ذاته، وإنما يستمد هذا الدخول عدم مشروعيته من كونه غير مصرح به[٩]. كما أن قضية اختراق المواقع الإلكترونية هي واحدة من القضايا التي تقع تحت طائلة القانون، والتي تندرج تحت قائمة الجرائم المعلوماتية، والاختراق بشكل عام هو: القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاصة بالهدف، وبالتالي يتعرض النظام المعلوماتي إلى الاختراق من قبل أفراد غير مصرح لهم بالدخول إليه أو البقاء فيه[١٠].

ووفقًا لنتائج إحصاءات " شبكة كاسبرسكي لأمن المعلومات" التي صدرت عن الربع الأول لعام ٢٠١٦م، فقد "ارتفع إجمالي عدد حالات الاختراق الإلكتروني المكتشفة من قبل منتجات "كاسبرسكي لاب" في الشرق الأوسط بنسبة ١٥% عما كانت عليه في الفترة ذاتها عام ٢٠١٥م، وعلى سبيل المثال، شهدت هجمات الفدية الخبيثة(Ransomware) التي تمكنت برامج كاسبرسكي لاب من اكتشافها ومنعها في الشرق الأوسط ارتفاعاً بنسبة ٦٧ %، وتأتي المؤسسات المالية ومؤسسات التجارة الإلكترونية والاتصالات والمؤسسات الحكومية في طليعة المؤسسات التي تُستهدف من قبل القراصنة الإلكترونيين عل مستوى المنطقة العربية[١١].

ومن أجل ما تقدم نجد المشرع المصري قد نص على جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة، في نص مستقل، وأقر لها عقوبة رادعة، وذلك بمقتضى نص المادة ٢٠ من قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨م، بأن جرم المشرع الولوج أو البقاء

---

(8) Bainbridge. D: Introduction to computer law, fourth edition, London, 2000, P.307.

(٩) د. أسامة بن غانم العبيدي، جريمة الدخول غير المشروع إلى النظام المعلوماتي: دراسة قانونية في ضوء القوانين المقارنة، بحث منشور في مجلة دراسات المعلومات، جمعية المكتبات والمعلومات السعودية، العدد ١٤، مايو ٢٠١٢م، ص١٣.

(١٠) د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، بهجان للطباعة والتجليد، مصر، ٢٠٠٩م، ص٢٣٥؛ د. عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولي، الطبعة الثانية، دار النهضة العربية، القاهرة، ١٩٩٥م، ص١٢٢ وما بعدها.

(11)David Emm and Others,"IT threat evolution in Q2 2016. Statistics", Kaspersky Lab detected, 11 AUG 2016, P.12. on the following website: https://securelist.com/it-threat-evolution-in-q2-2016-statistics/75640/,Accessed 25/12/2022 at 01.15 Pm.

غير المشروع أو تجاوز الحق في الولوج لموقع أو حساب أو نظام معلوماتي يخص الدولة أو أحد الأشخاص الاعتبارية العامة"[١].

يتضح من ذلك أن المشرع المصري جرم الاعتداء على الأنظمة الخاصة بالدولة، وهو ما لم ينص عليه الكثير من التشريعات في نص مستقل، فقد جعل المشرع المصري الدخول في أنظمة الدولة أو إحدى الأشخاص الاعتبارية العامة بقصد الاعتراض أو الحصول على معلومات يُشكل جناية وعقوبته السجن والغرامة.كما جرم المشرع المصري كذلك الاعتداء على سلامة الشبكة المعلوماتية، وذلك فيما قصت به المادة ٢١ من القانون المُشار إليه[٢].

وبذلك يكون المشرع المصري قد أسبغ حمايته على ما يُعتبر موقعًا أو بريدًا إلكترونيًا أو حسابًا خاصًا أو نظامًا معلوماتيًا يُدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكًا لها, أو يخصها، كما أسبغ المشرع المصري كذلك الحماية الجنائية ضد الاعتداء الذي يقع على الشبكة المعلوماتية، وليس الجهاز أو الأجهزة، ويظهر ذلك عندما شدد المشرع في العقاب على الاعتداء على الشبكة المعلوماتية، إذا ما كانت الشبكة تخص الدولة أو تديرها الدولة أو أحد الأشخاص الاعتباري العامة، إذ يصبح الفعل جناية كما هو الحال بالنسبة للشبكة العامة الإنترنت. كما حرص المشرع المصري على تجريم كل فعل ينطوي على اعترض يتم بدون وجه حق لأي معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها[٣]، الأمر الذي يفهم منه أن تلك الجريمة تنطبق إذا ما كان الاعتراض غير القانوني قد وقع على على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي الخاصة بالدولة، لا سيما وأن المشرع المصري قد أورد عبارة" أي معلومات أو بيانات".

كما يُلاحظ أنه يتحقق الإتلاف المنصوص عليه في المادة ٣٦١ من قانون العقوبات المصري، بإتلاف أو محو تعليمات البرامج أو البيانات ذاتها. حيث إن عدم انطباق وصف المال على البرامج والمعلومات يؤدي حتمًا إلى تجريده من الحماية القانونية الجنائية مما يفتح المجال واسعًا أمام قراصنة البرامج والمعلومات، الأمر الذي يدعونا للقول بأنه يتعين عدم الاكتفاء بتطبيق تلك النصوص بعمومها، بل يجب أن يتدخل المشرع بالنص على صلاحية هذه الأموال المعنوية لأن تكون محلًا لجرائم

---

(١) انظر: المادة ٢٠ من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨م.

(٢) المادة ٢١ من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨م.

(٣) المادة ١٦ من قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨م.

كالسرقة[١]، والإتلاف والنصب، وغيرها، أو إعطاء مفهوم واسع للمال كما فعلت بعض التشريعات[٢].

والعبرة في إتلاف الشيء هو إنقاص قيمته ولذلك فإن محل الحماية الحقيقي هو قيمة الشيء وليس حماية مادته إلا وسيلة لحماية قيمته، فإذا كان الفعل قد أفقد الشيء قيمته إذا نقص منها فقد حق الاعتداء الذي يعاقب عليه القانون باعتباره قد ذهب بأهمية الشيء بالنسبة إلى مالكه[٣]، وقد يتحقق الإتلاف المعلوماتي بوجه عام بصورتين: **الصورة الأولى:** تتمثل في إدخال بيانات أو معلومات في نظام الحاسب الآلي، والمُراد بذلك هو إدخال بيانات عن طريق شبكة الإنترنت في أحد المواقع والنظم المعلوماتية الخاصة بالدولة لم تكن موجودة من قبل، وذلك بغرض الإضرار بجهازه وإتلافه. **الصورة الثانية:** فتتمثل في محو أو تعديل بعض البيانات المخزنة بالحاسب الآلي، ومحو البيانات يعني تدميرها، أي إتلافها بصورة جزئية أو كلية والتعديل يعني التلاعب في هذه البيانات بشكل يؤثر في قيمتها بحيث يتحقق معنى الإتلاف [٤].

نخلص من ذلك أنه من خلال الإتلاف يقوم الجاني بتعييب الشيء على نحو يفقده قيمته الكلية أو الجزئية، أي أنه من الممكن أن يكون هناك إتلافًا للمال للمنقول يجرمه القانون إذا كان الفعل أفقد الشيء قيمته الكلية أو الجزئية، وبالنتيجة؛ فإن الإتلاف يتمثل بإعدام المنقول (مادته) أو إدخال تغييرات شاملة عليها من شأن هذه التغييرات أن تجعله غير صالح للاستعمال للغرض المخصص له وبذلك تضيع قيمته على المال، ذلك إن فعل التجريم يهدف إلى الحفاظ على حق الملكية الذي يمكن التوصل إليه بحماية موضوع المال نفسه أو الحفاظ على القيمة الاقتصادية للشيء التي تعتمد على صلاحيته للاستعمال[٥].

---

(1)Sevgi Kelci,"Vol, fraude et autres infractions semblables et Internet",Revue Lex Electronica , Vol.12,n°1 ,2007, P.7, disponible sur le site: http://www.lex-electronica.org/articles/v12-1/kelci.pdf Consulté le 12/01/2022 à 11h30.

(٢) د. عفيفي كامل عفيفي، جرائم الكمبيوتر، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت–لبنان، ٢٠٠٣م، ص١٤٢؛ د.سالم بن مبارك بن سليم اليعقوبي، الحماية الجنائية للأدلة المعلوماتية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ١٤٤٠ه/٢٠١٩م، ص١٠٠، ١٠١، وينظر كذلك:

Eric J. Sinrod, and William P Reilly, "Cyber- Crimes: A practical approach to the Application of Federal Computer Crimes Laws, 16 Santa Clara computer and High Tech L. J. 177, P.90, (2000).

(٣) د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، ١٩٩٢م، ص١٢٧.

(٤) د. هدى حامد قشقوش، الإتلاف العمدي لبرامج وبيانات الحاسب الإلكتروني، بحث مُقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، دولة الإمارات، الفترة من ١: ٣ مايو ٢٠٠٠م، ص٦٩.

(٥) د. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون: دراسة مقارنة، منشأة المعارف، الإسكندرية، بدون سنة نشر، ص١٩٨.

وفيما يتعلق بجرائم الاعتداء على النظم المعلوماتية الخاصة بالدولة؛ فإننا نجد أن هناك صوراً لإتلاف البرامج والمعلومات الخاصة بالدولة[1]، وتتمثل تلك الصور في: محو البيانات إلكترونياً بتدميرها أو جزء منها، وكذلك إدخال بيانات في نظام المعالجة الآلية لم تكن موجودة مما يؤدي إلى التشويش على صحة البيانات القائمة، كما تتمثل كذلك في تعديل البيانات أو تعديل طرق انتقالها، أو تعديل وسائل هذا الانتقال[2]. كما حظر المشرع على مقدمي الخدمة كل من الاعتراض والاختراق، فالاعتراض يشمل كل مشاهدة البيانات أو المعلومات أو الحصول عليها بغرض التنصت أو التعطيل، أو التخزين أو النسخ، أو التسجيل، أو تغيير المحتوى، أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه وذلك لأسباب غير مشروعة ودون وجه حق، والاختراق يشتمل على 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.

والقصد من كل ذلك حماية الأمن القومي الذي يتسع ولا يضيق ليتضمن كل ما يتصل باستقلال واستقرار وأمن الوطن ووحدته وسلامة أراضيه، وأمنه المالي والاقتصادي جزء لا يتجزأ من أمنه القومي، وكل ما يتعلق بشئون رئاسة الجمهورية ومجلس الدفاع الوطني ومجلس الأمن القومي، ووزارة الدفاع والإنتاج الحربي، ووزارة الداخلية، والمخابرات العامة، وهيئة الرقابة الإدارية، والأجهزة التابعة لتلك الجهات.

ويُلاحظ أن جرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة بكافة صورها تُعد من الجرائم المعلوماتية الواقعة على أمن الدولة، ونظامها المعلوماتي أي مجموعة الجرائم التي تمس بشكل مباشر سيادة الدولة، وأراضيها، ومواطنيها، أو تنال من نظام الحكم فيها، أو تعرض مؤسساتها للخطر، ونظراً لخطورة جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة، فقد رصد المشرع المصري لها العديد من العقوبات الصارمة في قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨م.

الفرع الثاني

جرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة في التشريع العماني والمقارن

---

(١) المادة ١٧ من قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨م.

(٢) د. عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الطبعة الأولى، دار الفكر الجامعي الإسكندرية، الإسكندرية، ٢٠٠٢م.

سبق وأن أشرنا إلى أن التشريعات المقارنة، ومن بينها التشريع العُماني لم يفرد لجريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة نصاً مستقلًا، وإنما نصت تلك التشريعات على عدة صور يمكن اعتبارها أنماطًا للجرائم الواقعة على الأنظمة المعلوماتية الخاصة بالدولة، غير إنه يمكن حصر هذه الصور التجريمية في الصور التالية:

أولًا: جريمة الدخول غير المشروع إلى النظام المعلوماتي:

يُعتبر مصطلح "الدخول غير المصرح به" مصطلح شائع الاستخدام في التشريعات التي تعاقب على هذه الجريمة، ويُسميها البعض "جريمة الدخول غير القانوني" (١)، وهناك من يطلق عليها "الدخول غير الشرعي"(٢)، بينما تستخدم تشريعات أخرى مصطلح "الدخول دون وجه حق"(٣)، والدخول دون مسوغ قانوني (٤)، ولا يُشترط أن يتم الدخول بوسيلة بعينها فكل الوسائل سواء، ويستوي أن يتم الدخول بشكل مباشر أو غير مباشر (٥). فالدخول يكون مصرحاً به عندما يملك الشخص الحق في الدخول للبيانات، أو عندما يمنح هذا الشخص السلطة بالدخول من شخص آخر يملك الحق بذلك، ويكون الدخول غير مصرح به إذا كان من له السيطرة على النظام قد وضع بعض القيود للدخول إليه ولم يحترم الجاني تلك القيود، أو كان يتطلب ضرورة دفع مبلغ من النقود وتم الدخول دون دفع ذلك المبلغ(٦)، وهي جريمة شكلية(٧)، وتشدد عقوبة الجريمة حال حصول نتيجة.

وما تجب الإشارة إليه أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات قد نصت على جريمة الاعتراض غير القانوني (٨). كما تم تجريم الاعتراض غير القانوني في القانون العماني(٩)، والكويتي(١٠) والسعودي(١١) والإماراتي(١)، وذلك بتجريم كل فعل ينطوي على اعتراض غير مشروع

---

(١) المادة ٢ من اتفاقية المجلس الأوربي بخصوص جرائم الإنترنت (اتفاقية بودابست لسنة ٢٠٠١)، التي فرضت على الدول الأطراف تبني الإجراءات التشريعية أو أية إجراءات أخرى ترى أنها ضرورية لتجريم الدخول بشكل قصدي غير القانوني في تشريعاتها الوطنية؛ سواء تم هذا الدخول لكل أو لجزء من نظام الحاسب.

(٢) المادة ٢ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة عن جامعة الدول العربية.

(٣) المادة ٣ قانون مكافحة جرائم تقنية المعلومات العماني.

(٤) المادة ٢ من قانون جرائم تقنية المعلومات البحريني رقم ٦ لسنة ٢٠١٤.

(٥) د. علي عبد القادر القهوجي، المرجع السابق، ص٥٩٩.

(٦) د. علي عبد القادر القهوجي، المرجع السابق، ص٦٠٠.

(٧) د. أحمد شوقي عمر أبو خطوة، المبادئ العامة في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، ٢٠١٣م، ص١٥٦.

(٨) المادة السابعة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

(٩) المادة ٨ من قانون مكافحة تقنية المعلومات العُماني رقم ١٢ لسنة ٢٠١١م.

(١٠) المادة ٢ من القانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات الكويتي.

(١١) الفقرة الأولى من المادة الثالثة من نظام مكافحة جرائم تقنية المعلومات السعودي.

ومتعمد للبيانات والمعلومات المتداولة بوسائل التقنية المعلوماتية، أو الاعتراض غير المشروع والمتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات، ويختلف الاعتراض غير القانوني أو ما يُعرف بالاعتراض غير المشروع عن الدخول غير المصرح به في أن الدخول يفترض تشغيل النظام، أما الاعتراض فإنه يكون تشغيل النظام قد تم عن طريق شخص آخر(٢). أما البقاء غير المشروع يُقصد به التواجد داخل النظام المعلوماتي خلافاً لإرادة من له الحق في منح الإذن في التواجد في النظام"(٣).

ويكون ذلك إما في الأحوال التي يكون فيها الدخول مشروعاً كوجود تصريح للدخول على سبيل المثال، أو لأن الدخول غير معاقب عليه وذلك لانتفاء عنصر من عنصر التجريم وتتحقق الصورة الأولى كوجود تصريح للدخول إلى النظام المعلوماتي لوقت محدد إلا أن هذا الوقت ينتهي ومع ذلك يظل الشخص داخل النظام(٤). فالبقاء في هذا الفرض يتحقق عند عدم قطع الشخص بالاتصال بالنظام رغم إدراكه وعلمه أن وجوده في النظام غير مشروع لانتهاء وقت التصريح، فالجريمة تقوم من اللحظة التي كان يجب على الشخص أن يخرج فيها من النظام ولا يقوم فيها بالخروج منه(٥).

وتتحقق الصورة الثانية لقيام جريمة البقاء غير المصرح به في الأحوال التي يكون فيها الدخول عن طريق الخطأ أو عن طريق الصدفة، إلا أن الفاعل رغم اكتشافه ذلك يظل في النظام ولا يخرج منه، فكما هو معلوم أن جريمة البقاء غير المصرح به هي الأخرى إلى جانب جريمة الدخول غير المشروع تعتبر جريمة عمدية ولا ترتكب بصورة الخطأ ومن هنا جاءت الأهمية لتجريم جريمة البقاء غير المشروع لمواجهة هذين الفرضين(٦). كما أن البقاء في هذا الفرض يبدأ أيضاً من اللحظة التي يعلم فيها الشخص أن دخوله غير مشروع ومع ذلك يبقى في النظام ولا يضع حداً لوجوده(٧).

نخلص من ذلك إلى أنه قد يتحقق البقاء المعاقب عليه داخل النظام المعلوماتي مستقلًا عن الدخول على النظام، وقد يجتمعان، ويكون البقاء معاقبًا عليه استقلالًا حين يكون الدخول إلى النظام مشروعًا، ويكون هكذا في حالتين:

---

(١) المادة ١٢ من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم الإلكترونية الإماراتي.

(٢) د. أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، ط١، دار النهضة العربية، القاهرة، ٢٠١٠م، ص٢٥٩.

(٣) د. محمود أحمد طه، المواجهة التشريعية والإنترنت: دراسة مقارنة، دار الفكر والقانون، المنصورة، ٢٠١٧م، ص٣٠.

(٤) د. عبد الإله محمد النوايسة، جرائم التجسس الإلكتروني في التشريع الأردني: دراسة تحليلية، مجلة دراسات-علوم الشريعة والقانون، عمادة البحث العلمي، الجامعة الأردنية، المجلد ٤٦، ملحق، ٢٠١٩م، ص٢٣٤.

(٥) محمد خليفة، الحماية الجنائية لمعطيات الحاسوب الآلي، الطبعة الأولى، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٧م، ص١٥٤.

(٦) د. عبد الإله محمد النوايسة وآخرين، المرجع السابق، ص٢٣٤-٢٣٥.

(٧) محمد خليفة، المرجع السابق، ص١٥٥.

الحالة الأولى: إذا تم الدخول إلى النظام بمصادفة أو عن طريق الخطأ أو السهو، إذ كان يجب في هذه الحالة على المتدخل أن يقطع وجوده وينسحب فوراً فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع متى ثبت في حقه تعمده البقاء. **الحالة الثانية:** إذا تجاوز المتدخل المدة المسموح بها للبقاء بداخل النظام أو حصل المتدخل بصورة مشروعة على الخدمة مدة أطول من المدة التي دفع مقابلها نتيجة استخدام وسائل أو عمليات غير مشروعة.

وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معاً وذلك في الفرض الذي لا يكون فيه الجاني الحق في الدخول إلى النظام، ويدخل إليه فعلًا ضد إرادة من له حق السيطرة عليه، ثم يبقى داخل النظام بعد ذلك، وإن كانت جريمة البقاء غير المشروع إلى النظام المعلوماتي لا تصدر من الفاعل في جريمة الدخول، وذلك لأن تجريم البقاء من قُبيل النص الاحتياطي بالنسبة لتجريم التداخل فلا تسبب جريمة البقاء إلى من قام بالتداخل غير المشروع شأنها في ذلك شأن جريمة إخفاء الأشياء المسروقة. فلا تصدر من مرتكب جريمة السرقة[١]، **ومن وسائل وأسباب اختراق النظام المعلوماتي للدولة، ما يلي:**

أ. الرغبة في تدمير المواقع الإلكترونية الخاصة بالدولة:

ويرجع ذلك إلى الرغبة في تدمير الموقع الإلكتروني الذي يقصد به الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالإنترنت من خلال نظام آلي **(server–pc)** أو مجموعة نظم مترابطة شبكيا بهدف تخريب نقطة الاتصال أو النظام[٢]، ومن الوسائل المستخدمة لتدمير المواقع ضخ مئات الآلات من الرسائل الإلكترونية من جهاز الحاسوب الخاص بالمعتدي إلى الموقع الحكومي المستهدف للتأثير على السعة التخزينية للموقع فتشكل هذه الكمية الهائلة من الرسائل الإلكترونية ضغطًا يؤدي في النهاية إلى تفجير الموقع العامل على الشبكة وتشتيت البيانات والمعلومات المخزنة في الموقع فتنتقل إلى جهاز المعتدي[٣].

ب. الرغبة في تشويه المواقع الخاصة بالدولة:

يوجد تشابه كبير، بين ما يحصل في العالم الافتراضي من عمليات تشويه مواقع الويب، وبين ما يحدث على أرض الواقع عندما يتم إنزال علم دولة معينة، من السفينة، ورفع علم القراصنة مكانه، حيث أن عملية التشويه، في أغلب الأحيان، ليست سوى تغيير الصفحة الرئيسية للموقع، بصفحة

---

(١) د. محمود أحمد طه، المرجع السابق، ص٣١.

(٢) د. حسين بن سعيد بن سيف الغافري، الجرائم الواقعة على التجارة الإلكترونية، مسقط، سلطنة عُمان، ٢٠٠٦م، ص٥٢.

(٣) د. عبد الرحمن بن عبد الله السند، وسائل الإرهاب الإلكتروني "حكمها في الإسلام وطرق مكافحتها"، بحث مقدم للمؤتمر العالمي عن موقف الإسلام من الإرهاب، جامعة الإمام محمد بن سعود الإسلامية، المملكة العربية السعودية، ٢٠٠٤م، ص١٦-١٧.

أخرى، يعلن المخترق فيها انتصاره على نظام مزود ويب والإجراءات الأمنية للشبكة، ويقصد من ورائها إبراز قدراته التقنية، وإعلان تحديه للمشرفين على نظم مزودات ويب، ليثبت لنفسه، أو لغيره امتلاكه المقدرة التقنية على كسر نظام الحماية في هذه المزودات، الأمر الذي يتطلب معرفة معمقة لطريقة عمل الإنترنت، وبروتوكولات التشبيك، وأنظمة التشغيل المختلفة التي تعمل عليها مزودات ويب، وتتضمن الصفحة الجديدة أحياناً رسالة يرغب الشخص الذي قام بعملية التشويه إيصالها للعالم، وقد تتضمن هذه الرسالة اعتراضاً منه على حالة سياسية أو اجتماعية، أو صرخة يريد إيصالها، إلى كل من يزور هذا الموقع(١).

وتقتصر الأضرار التي تتسبب بها عمليات تشويه مواقع ويب، على الإضرار بسمعة الجهة المالكة للموقع، حيث يتم تغيير الصفحة الرئيسية فقط من الموقع بصفحة HTML من تصميم المخترق، ولا يلجأ المخترقون عادة في عمليات التشويه إلى تدمير محتويات الموقع، حيث يستطيع الآخرون زيارة المواقع التي تتعرض لعمليات التشويه والوصول إلى جميع صفحاته المكونة للموقع. كما يتبع المخترقون عادة أساليب عدة في عمليات تشويه صفحات ويب، وتختلف هذه الأساليب من موقع إلى آخر، بناءً على نوع نظام التشغيل، ومزود ويب الذي يعتمد عليه الموقع، وهنا نذكر أكثر من هذه الأساليب انتشاراً وهي:

١. **الدخول بهوية مخفية (anonymous) عبر منفذ بروتوكول FTP(٢):** تمكن تلك الطريقة المخترق في بعض الحالات من الحصول على ملف كلمة الدخول المشفرة الخاصة بأحد المشرفين على الشبكة، أو من يملكون حق تعديل محتويات الموقع، والعمل على فك تشفيرها، فمن شأن حصول المخترق على كلمة السر الخاصة لأحد المشرفين، السماح له بالدخول إلى مزود ويب، وتغيير الصفحة الرئيسية، ويلجأ المخترقون، بعد الحصول على ملف كلمة السر، على استخدام برامج خاصة لتخمين كلمات السر.

٢. **استغلال الثغرات الأمنية في مزودات ويب، وأنظمة التشغيل:** لا ريب في أنه لا يوجد أي نظام تشغيل، أو مزود ويب يخلو من ثغرات أمنية تعرض مستخدميه لخطر الاختراق – حتى ولو كانت الدولة نفسها–، لذلك يعمل المطورون بشكل مستمر على سد هذه الثغرات كلما اكتشفت، غير إنه يستغل الهكرة هذه الثغرات الأمنية في عمليات الاختراق، إلى أن تجد الشركة المصممة للنظام الحل المناسب لها، وتبقى بعض الثغرات متاحة لفترة طويلة

---

(١) د. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت: دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٠٩م، ص٥٥.

(٢) د. محمد سليمان الخوالدة، جريمة الدخول غير المشروع إلى موقع إلكتروني أو نظام معلومات وفق التشريع الأردني: دراسة مقارنة"، رسالة ماجستير، كلية الدراسات العليا، الجامعة الأردنية، ٢٠١٢م، ص٣٣.

حتى يتم اكتشافها، وذلك لأن أغلب الثغرات التي يكتشفها الهكر، لا يعلنون عنها بسرعة، ليتمكنوا من استغلالها فترة أطول، وبالتالي ينبغي على جميع مدراء ومشرفي الشبكات، متابعة مواقع الشركات المصممة لنظم التشغيل، ومزودات ويب، ليتسنى لهم الاطلاع على آخر ما تم التوصل إليه من ثغرات أمنية، وجل برامج الترقيع (patches) لها، حيث تحرص هذه الشركات على تقديم مثل هذه البرامج بأسرع وقت ممكن[١].

ج. حجب الخدمة:

ويقصد بذلك تحكم القراصنة والعابثين الإلكترونيين لمهاجمة مواقع الإنترنت عن بعد لإرسال تلك البيانات إلى المواقع بشكل كثيف مما يسبب بطء الخدمات أو زحاماً مرورياً بهذه المواقع، ويسبب صعوبة وصول المستخدمين لها نظراً لهذا الزحام[٢].

د. الحصول على بيانات تمس الأمن القومي أو الاقتصاد الوطني:

من الممكن ارتكاب هذه الجريمة بقصد الحصول على بيانات تمس الأمن القومي أو الاقتصاد الوطني، وفي هذا الفرض يقصد الجاني من التداخل الحصول على بيانات تمس الأمن القومي، أو الاقتصاد الوطني [٣].

ولقد نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على جريمة الدخول غير المشروع إلى النظام المعلوماتي نظراً لأهميتها غير إنه يلاحظ أن الاتفاقية قد نصت على كل من جريمة الدخول غير المشروع والبقاء غير المشروع وكذلك جريمة تجاوز حدود التصريح ولعل ما يؤكد الجريمة الأخيرة عبارة "..... وكل اتصال غير مشروع... أو الاستمرار به" الواردة في الفقرة رقم ١ من المادة السادسة، بالإضافة إلى جريمة الاعتراض غير القانوني وذلك في المادة السابعة [٤].

ولقد جرم قانون مكافحة جرائم تقنية المعلومات العماني هذه الجريمة وذلك في المادة رقم (٣) من قانون مكافحة جرائم تقنية المعلومات رقم ١٢ لسنة ٢٠١١م التي نصت على أنه:" يُعاقب بالسجن مدة لا تقل عن شهر... كل من دخل عمداً ودون وجه حق... أو تجاوز الدخول المصرح به إليها أو استمر فيها بعد علمه بذلك". كما تم تجريم هذه الجريمة بكافة صورها في التشريع الكويتي[٥]،

---

(١) د. محمد سليمان الخوالدة، المرجع السابق، ص٣٤.

(٢) حسين بن سعيد، الجرائم الواقعة على التجارة الإلكترونية، سلطنة عمان، مسقط ٢٠٠٦م، على الرابط:
http://www.mohamoon.com/montada/default.aspx?Action=Display&ID=106198&Type=3

(٣) د. محمود أحمد طه، المرجع السابق، ص٢٥.

(٤) انظر: المادتان السادسة والسابعة من الاتفاقية.

(٥) المادة ٢ من القانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات الكويتي.

والسعودي[١]. كما نجد أن المشرع الفرنسي قد جرم الدخول غير المشروع إلى نظام معالجة معطيات البيانات الآلية في المادة ١/٣٣٢ من قانون العقوبات الفرنسي الجديد، ولقد أشارت اللجنة القانونية في البرلمان الإنجليزي الداعية لتجريم الدخول غير المصرح به المجرد في قانون إساءة استخدام الكمبيوتر لسنة ١٩٩٠م، وأول هذه الأسباب الخسائر والتكاليف الحقيقية التي يتم تكبدها من قِبل أنظمة المعلومات التي تخترق أنظمتها الأمنية، كما يُمكن أن يكون مرحلة تمهيدية لارتكاب جرائم أخرى[٢].

ويُلاحظ أن جميع التشريعات المقارنة تتفق فيما بينها في العديد من الجوانب والنصوص التشريعية فيما يتعلق بالنص على هذه الجريمة، مع وجود بعض الأوجه الخلافية الضئيلة التي لا تؤثر على الجوانب الاتفاقية منها، ومن هذه النواحي الخلافية نذكر منها ما يلي:

أولًا: لم يتطرق كل من المشرع العُماني ونظيره الكويتي والسعودي إلى فعل البقاء المتعمد الذي يتحقق في حالة الدخول غير المشروع أو الدخول المشروع إلى أنظمة التقنية المعلوماتية رغم انتهاء الفترة المقررة لدخول الجاني والبقاء داخل النظام، على عكس ما اتبعه المشرع المصري ووفقًا لما هو وارد في المادة السادسة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات [٣].

ثانيًا: جعل المشرع المصري جعل من فعل البقاء المتعمد في حالة الدخول المشروع وتجاوز هذا الحق في الدخول بالبقاء بعد فوات المواعيد جريمة مستقلة وأوردها في مادة مستقلة، وقرر له عقوبة مغايرة أقل حدة وتشدد عن سابقتها من جريمة الدخول غير المشروع[٤].

ثالثًا: توسع المشرع الكويتي في ذكر وتعداد أوجه التعدي التي تُرتكب من خلال فعل الدخول غير المشروع والتي اعتبرها جريمة في حد ذاتها تستوجب التشديد، ومن قبيل هذا التوسع أنه جرم فعل التزوير أو الإتلاف لمستند أو سجل أو توقيع إلكتروني يحدث نتيجة الدخول غير المشروع[٥]، وهو ذات ما أورده المشرع الإماراتي حينما نص على جريمة تزوير مستند حكومي أو غير حكومي، وضاعف من حد العقوبة في حالة استعمال هذا المستند مع علم الجاني بتزويره، مع اختلاف أن المشرع الإماراتي لم يقرنه بجريمة الدخول غير المشروع، فقرر لها عقوبة رادعة سواء ارتكبت من خلال دخول مشروع أو غير مشروع. وتشدد أكثر من ذلك في حالة إذا ما وقع هذا التزوير على مستند رسمي أو بنكي أو مستندات حكومية. فقد نص المشرع الإماراتي على أن:"

---

(١) المادة ٢/٣، ٣ من نظام مكافحة جرائم تقنية المعلومات السعودي.

(2) International Solution, 27 Tex. Int. L.J. (1992). P496-497, Indicated by Dr. Rizgar Kadir Sharia & Law, Issue No. 40- October 2009, p. 48.

(٣) المادة السادسة من الاتفاقية.

(٤) المادة ١٥ من قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨م.

(٥) المادة ٢/٣ من قانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات الكويتي.

١- يُعاقب بالسجن المؤقت والغرامة التي لا تقل عن (١٥٠،٠٠٠) مائة وخمسون ألف درهم ولا تزيد على (٧٥٠،٠٠٠) سبعمائة وخمسون ألف درهم كل من زور مستنداً إلكترونياً من مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية أو المحلية.

٢- وتكون العقوبة الحبس والغرامة لا تقل عن (١٠٠،٠٠٠) مائة ألف درهم ولا تزيد على (٣٠٠،٠٠٠) ثلاثمائة ألف درهم، أو بإحدى هاتين العقوبتين، إذا وقع التزوير في مستندات جهة غير تلك المنصوص عليها في البند (١) من هذه المادة.

٣- ويعاقب بذات العقوبة المقررة لجريمة التزوير، بحسب الأحوال، من استعمل المستند الإلكتروني المزور مع علمه بتزويره[١].

كما نص المشرع الكويتي على جريمة النصب أو الاحتيال الإلكتروني إذا ما تم الاستيلاء للنفس أو للغير – بطرق احتيالية أو اسم كاذب أو انتحال صفة – على مال أو منفعة أو مستند أو توقيع على مستند، من خلال شبكة المعلومات أو باستخدام وسيلة تقنية[٢]، وهو خلافًا لما اتبعه المشرع السعودي الذي تناول جريمة النصب أو الاحتيال الإلكتروني في مادة مستقلة منه ولم يجعلها حالة من حالات تشديد العقوبة[٣]، وهو ذات ما فعله المشرع الإماراتي[٤]، والعُماني[٥]، وعلى العكس من ذلك فلم نجد لهذه الحالات مثيلًا بنصوص التشريع المصري الذي جاء خاليًا من ذكرها. كما تناول المشرع الكويتي فعل آخر يعد من الانتهاكات الخطيرة والمجرمة وهو حالة استخدام شبكة المعلومات أو أية وسيلة تقنية في التهديد أو الابتزاز لحمل الشخص على ارتكاب فعل أو الامتناع عنه، سواء أكان هذا التهديد بجناية أو مساس بكرامة الأشخاص أو خدشًا للشرف والاعتبار أو السمعة[٦]، وهو ذات ما أورده المشرع السعودي[٧] حتى وإن كان هذا الفعل مشروعًا.

والخلاصة أن المشرع الكويتي كان موفقًا وأكثر توفيقًا وحظًا من غيره في صياغة النصوص التشريعية لجريمة الدخول غير المشروع عن التشريعين المصري والعُماني وكذلك التشريعات العربية المقارنة، الأمر الذي نقترح معه ضرورة أن تتبنى تلك التشريعات ما ورد بنصوص التشريع

---

(١) المادة ١٤ من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم الإلكترونية الإماراتي.

(٢) المادة ٣/٥من قانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات الكويتي.

(٣) الفقرة الثانية من المادة الرابعة من نظام مكافحة جرائم تقنية المعلومات السعودي.

(٤)المادة ٤٠ من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم الإلكترونية الإماراتي.

(٥) المادة ١٢ من قانون مكافحة تقنية المعلومات العُماني.

(٦) المادة الرابعة من قانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات الكويتي.

(٧) الفقرة الثانية من المادة الثالثة من نظام مكافحة جرائم تقنية المعلومات السعودي.

الكويتي، وذلك بالتوسع في إدراج مثل هذه الحالات المتعلقة بتشديد العقوبة والمقترنة بجريمة الدخول غير المشروع.

ثانيًا: جريمة التجسس المعلوماتي:

يُعرف التجسس الإلكتروني بأنه دخول الجاني إلى الشبكة المعلوماتية أو نظام المعلومات أو موقع إلكتروني للحصول على محتوى إلكتروني غير متاح للجمهور يمس الأمن الوطني أو العلاقات الخارجية للدولة أو السلامة العامة أو الاقتصاد الوطني، مما من شأنه يؤدي إلى ارتكاب جريمة من الجرائم الواردة في قانون مكافحة جرائم تقنية المعلومات بوسيلة إلكترونية(١).

ونظرًا لظهور عصر المعلومات والاتصالات والازدهار تحولت وسائل التجسس والتنصت من الطرق التقليدية إلى الطرق الإلكترونية، لا سيما مع استخدام شبكة الإنترنت وانتشارها الواسع عربيًا وعالميًا. غير أنه لا تكمن الخطورة في استخدام شبكة الإنترنت، ولكن في ضعف الوسائل الأمنية المستخدمة في حماية الشبكات الخاصة بالمؤسسات والهيئات الحكومية، واعتمادها على وسائل حماية إنتاج شركات أجنبية يعرف معظم خبراء الشبكات والمعلومات أدق جوانبها الأمنية، وبالتالي لا يمكن الوثوق به(٢).

ولا يقتصر خطر الاختراق للشبكات والأنظمة والمواقع الخاصة بالدولة على المخترقون **HACKERS** أو ما يُعرف بمنظمات عامل الإنترنت السفلى التي تحاول دائمًا توجيه الاختراقات نحو أنظمة وشبكات ومواقع في العالم أجمع، فمخاطر هؤلاء محدودة، وتقتصر غالبًا على العبث وإتلاف المحتويات والتي يمكن التغلب عليها إذا وجدت نسخ احتياطية من البيانات والمعلومات، وإنما يمكن الخطر الحقيقي في عمليات التجسس التي تقوم بها الأجهزة الاستخباراتية للحصول على أسرار أو معلومات الدولة، ومن ثم؛ إفشاءها لدول أخرى تكون عادة معادية لها، أو استغلالها بما يضر بالمصلحة الوطنية للدولة(٣).

ويُعرف التجسس عمومًا بأنه:" السعي الذي يقوم به الأجنبي لجمع الوثائق والمعلومات السرية حول الموارد العسكرية وتنظيمات الدولة الهجومية أو الدفاعية ووضعها السياسي أو الاقتصادي بقصد تسليم هذه الوثائق والمعلومات إلى حكومة أجنبية مجانًا أو لقاء منفعة مالية(٤). كما يُعرف بأنه:" كل

---

(١) قصي أيمن البداودة، المسؤولية الجزائية الناشئة عن نشر وثائق الدولة عبر المواقع الإلكترونية، رسالة ماجستير، كلية الحقوق، جامعة الإسراء الخاصة، الأردن، ٢٠١٩م، ص٢٨، ٢٩.

(٢) د. ممدوح عبد الحميد عبد المطلب، جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية، مكتبة دار الحقوق، الشارقة، دولة الإمارات العربية المتحدة، ٢٠٠١م، ص٣٠.

(٣) د. نور سليمان يوسف يعقوب البالول، المرجع السابق، ص٣٥٧.

(٤) د. ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص٣١.

نشاط يقوم به أجنبي يكون من شأنه انتهاك أو خرق قواعد المحافظة التي تحيط بالأسرار المتعلقة بالدفاع الوطني"[١]. أما التجسس المعلوماتي فهو يتجسد في الاستحواذ بدون وجه مشروع وقانوني على معلومات ذات أهمية لا سيما فيما يتعلق بأمن الدولة، وكذلك الاستحواذ بدون وجه مشروع وقانوني على أسرار التعامل التجاري والتقنية الصناعية بجميع صورها[٢].

ولقد تحولت طرق التجسس في عصر المعلومات إلى عمليات تجسس إلكتروني، واختراق الأنظمة وشبكات الدول بعضها بعضاً، فمعظم الدول تحتفظ بوثائقها السرية مخزنة بهيئة رقمية في مزودات سرية، وتفيد تقارير عدة عن وجود العديد من حالات التجسس الدولي منها على سبيل المثال ما اكتشف أخيراً عن مفتاح وكالة الأمن القومي الأمريكية، والتي قامت بزراعته في نظام التشغيل ويندوز أحد منتجات شركة مايكروسوفت الأمريكية[٣].

ويمكن أن يتخذ التجسس المعلوماتي عدة صور، نذكر منها ما يلي: -

أ. **التجسس الإلكتروني بواسطة الكمبيوتر والإنترنت:** حيث أصبح الكمبيوتر والإنترنت أحد أهم وسائل التجسس المعلوماتي استخداماً، وأضحى الإنترنت الرابط الذي يمكن جهاز حاسب ما وبواسطة تقنيات خاصة تتطور باستمرار من الاختراق والحصول على المعلومات الموجودة في جهاز آخر أو تعديلها أو حذفها، أو إتلافها، أو الاطلاع عليها أو إفشائها، ولكها تُعد سلوكيات مكونة لجريمة التجسس المعلوماتي[٤].

ب. **التجسس المعلوماتي بواسطة الهاتف:** فقد تزايدت أنشطة الاختراق لخطوط الهاتف من جهة، ومن جهة أخرى يُستخدم الهاتف كوسيلة فعالة للتجسس بالنظر إلى تعدد التقنيات والبرمجيات الحديثة والخصائص التي تمتاز بها الهواتف النقالة[٥].

ج. **التجسس بواسطة البريد الإلكتروني:** إذ يقوم الجاني في تلك الصورة بزرع أحصنة طروادة، وكذلك عن طريق إنزال بعض البرامج من أحد المواقع غير الموثوق بها، وكذلك

---

(١) د. محمود سليمان موسى، التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة، دار المطبوعات الجامعية، الإسكندرية، ٢٠١٤م، ص١١٢.

(٢) د. سليمان عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الإنترنت، منشورات الحلبي الحقوقية، بيروت، ٢٠١١م، ص٣٢٥.

(٣) د. سعد إبراهيم الأعظمي، جرائم التجسس في التشريع العراقي: دراسة مقارنة، د.ن، ١٩٨١م، ص١٥.

(٤) د. نادية سلامي، التجسس الإلكتروني كأثر للاستخدام غير المشروع للفضاء الإلكتروني على أمن الدولة الخارجي، بحث منشور في مجلة دراسات، جامعة عمار ثليجي بالأغوط، الجزائر، العدد ٥٦، يوليو ٢٠١٧م، ص٢٤١.

(٥) د. علي عدنان الفيل، الإجرام الإلكتروني، الطبعة الأولى، منشورات زين الحقوقية، بيروت، لبنان، ٢٠١١م، ص٩٦، ٩٧؛ عدلي محمد عبد الكرخي، جريمة الإرهاب عبر الوسائل الإلكترونية في القانونين اللبناني والعراقي، رسالة ماجستير، كلية الحقوق والعلوم السياسية، الجامعة الإسلامية في لبنان، ٢٠١٨م، ص٧٠.

يمكن إعادة تكوين حصان طروادة من خلال الماكرو الموجودة ببرامج معالجات النصوص، كما يمكن للجاني استخدام الفيروسات في الاختراق والتجسس المعلوماتي، ومن أهم القضايا التي يمكن الإشارة في هذا الصدد قضية "**ويكيليكس**"(١).

د. **التجسس عن طريق كسر كلمات السر:** وذلك عن طريق معرفة كلمة السر، وكلمة السر هنا بمثابة مفتاح لتأمين البيانات، ويقوم المجرم المعلوماتي بكسرها والطريقة الأولية لذلك هي مجرد التجريب، ونتيجة لتوقعهم لوجود كلمة سر من طبيعة خاصة سواء تمثل ذلك في حروف أو تواريخ أو أرقام كذلك قد يتمثل تكنيك كسر كلمات السر في استخدام برامج الغرض منها فض السرية(٢).

ه. **التجسس عن طريق انتحال الشخصية:** وتتمثل هذه الطريقة في أن الجاني ينتحل شخصية لآخر، ومن خلال ذلك يصل إلى علمه ما يبحث عنه من بيانات، وأشهر أمثلة على ذلك أن ينتحل شخص شخصية التجار في عملية تجارة إلكترونية، ويحصل على أرقام بطاقة العميل ليحصل منها مبالغ عن عمليات وهمية أو أن يحصل على بيانات خاصة بصفقات تجارية مما يدخل في نطاق التحايل المعلوماتي(٣).

ويعتمد التجسس المعلوماتي أساساً في عملية التجسس على برنامج موجه يؤدي عمله في التجسس بناءً على أوامر داخلية صادرة عنه، بمعنى أن يقوم باكتشاف ثغرة أو نقطة ضعف أمنية في النظام الإلكتروني، ومن خلالها يفتح نفاذة للتجسس على البيانات والملفات المخزنة داخل الحاسب الآلي، ويوصلها إلى الجاني عن طريق حاسبه بحيث يوجه الجاني أوامره مباشرة لجهاز المجني عليها عن طريق البرنامج المخفي، وهو نفس فكرة الفيروس المعلوماتي الذي يختبئ، ثم ينشط، ويبدأ عمله الهجومي(٤).

---

(١) تعود تفاصيل هذه القضية حول قيام الأسترالي جوليان أسانج عام ٢٠١٠م في النشر على موقعه "ويكيليكس" معلومات سرية ألحقت ضرراً ملموساً بسمعة الحكومة الأمريكية، وخوفًا من تسليمه إلى الولايات المتحدة ومحاكمته هناك لجأ في عام ٢٠١٢م إلى سفارة الإكوادور في لندن، وبينما صدرت بحقه مذكرة توقيف في ستوكهولم منحته الإكوادور حق اللجوء السياسي، وقد اعترت هذه القضية إحدى عوارض مشكلة جديدة كانت نتيجة التقدم التكنولوجي الذي سمح بسرقة كمية ضخمة من البيانات، وبتكلفة متدنية أو بدون تكلفة من طرف أو أكثر لتنشر حصريًا على الخط. يُراجع في ذلك تفصيلًا:

Tim Maurer,"WikiLeaks 2010: A Glimpse of the Future?",Science, Technology, and Public Policy Program Explorations in Cyber International Relations Project,Belfer Center for Science and International Affairs,Harvard Kennedy School,Cambridge, USA, 2011.

(٢) د. هدى حامد قشقوش، السياسة الجنائية لمواجهة الجريمة المعلوماتية، دار النهضة العربية، القاهرة، ٢٠١٢م، ص٧١.

(٣) المرجع السابق، ص٧٢.

(٤) د. هدى حامد قشقوش، المرجع السابق، ص٦٠.

ويرى الباحث أن الطرائق الفنية للتجسس المعلوماتي سوف تكون أكثر الطرائق استخداماً في المستقبل من قبل التنظيمات الإرهابية، نظراً لأهمية المعلومات الخاصة بالمؤسسات والقطاعات الحكومية، وخصوصاً العسكرية والسياسية والاقتصادية، وهذه المعلومات إذا تعرضت للتجسس، وتم الحصول عليها، فسوف يُساء استخدامها من أجل الإضرار بمصلحة المجتمع والوطن على حد سواء.

ثالثًا: جريمة الإتلاف والتدمير المعلوماتي:

يُعرف الإتلاف–بوجه عام–اصطلاحاً بأنه تخريب الشيء محل الجريمة، بإتلافه أو التقليل من قيمته، وذلك بجعله غير صالح للاستعمال أو تعطيله، أي أنه تعييب الشيء على نحو يفقده قيمته الكلية أو الجزئية (١). بحيث يذهب أو تقل قيمته الاقتصادية (٢). بينما يُعرف الإتلاف المعلوماتي بأنه محو المعلومات أو البرامج كلياً أو تدميرها إلكترونياً أو أن يتم تشويه المعلومات أو البرنامج على نحو فيه إتلاف يجعلها غير صالحة للاستعمال (٣). كما يُعرف كذلك بأنه:" إتلاف أو محو تعليمات البرامج أو البيانات ذاتها ويطلق عليه مصطلح تدمير نظم المعلومات، وعادة لا يستهدف مرتكب هذه الاعتداء فائدة مالية لنفسه، بل يسعى للإعاقة وتعطيل نظم المعلومات عن أداء وظائفها وإحداث أضرار بها(٤).

كما يُلاحظ أن الإتلاف المعلوماتي هو تخريب الشيء موضوع الجريمة، وذلك بجعله غير صالح للاستعمال أو الانتفاع به، أو كذلك التقليل من منفعته، وبمعنى آخر فإن الإتلاف لا يخرج عن كونه فناء للشيء أو جعله بحالة غير الحالة التي هو عليها بحيث لا يمكن الاستفادة منه وفقًا للغرض الذي وجد من أجله، مما يعني أن جوهر الإتلاف هو إفقار المال المتلف منفعته أو صلاحيته للاستعمال في الغرض الذي وجد من أجله، أو هو التأثير على مادة الشيء على نحو يذهب أو يقلل من قيمته الاقتصادية عن طريق الانتقاص من كفاءته لأوجه الاستعمال المعد لها(٥).

ويوجد للإتلاف المعلوماتي للأنظمة المعلوماتية الخاصة بالدولة صوراً وأشكال متعددة أخرى، فمنها ما يؤثر على ماديات النظام المعلوماتي بتعطيلها وإيقافها عن العمل بالطرق المادية بالكسر

---

(١) د. يوسف بن سعيد بن محمد الكلباني، الحماية الجزائية للبيانات الإلكترونية في التشريعين العماني والمصري، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق–جامعة عين شمس، ١٤٣٧هـ/٢٠١٦م، ص١٣٦.

(٢) د. محمد نصر محمد عوض القطري، الإشكاليات القانونية لحماية سلامة المعلومات: دراسة تطبيقية على الحماية الجنائية من الإتلاف المعلوماتي، بحث منشور في مجلة الفكر الشرطي، القيادة العامة لشرطة الشارقة، مركز بحوث الشرطة، دولة الإمارات العربية المتحدة، المجلد ٢٤، العدد ٩٣، أبريل ٢٠١٥م، ص١٣٩.

(٣) د. مدحت محمد عبد العزيز إبراهيم، الجرائم المعلوماتية الواقعة على النظام المعلوماتي: دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠١٥م، ص٩٥.

(4) Walter Gary Sharp, Redefining National Security in Today's World of information technology and Emergent Threats, 9 Doke J Comp and Int'l,1999, P.383-384,

(٥) د. محمود محمود مصطفى، شرح قانون العقوبات القسم الخاص، الطبعة الثامنة، دار النهضة العربية، القاهرة، ١٩٨٤م، ص٦٤٥.

والتخريب إلى غير ذلك من الطرق، وأيضًا استخدام الطرق التقنية في الإتلاف المعلوماتي[١]، نذكر من ذلك ما يلي:

أ. **الاعتداء على المعلومات مما يؤدي إلى إعاقة وتعطيل النظام عن العمل:** إذ ينجم عن فعل يتسبب في تباطؤ أو ارتباك عمل نظام المعالجة الآلية للمعلومات، ويترتب على ذلك تغير في حالة عمل النظام. ويسوي بعضهم بين عرقلة النظام عن العمل ومحو أو تعديل أو إلغاء المعلومات، وحتى يمكن أن تتحقق الفاعلية في الإتلاف ينبغي أن يوجه لبرامج تشغيل النظام المعلوماتي، وليس على المعلومات بالمعنى الضيق، سواء أكان نظام التشغيل يتعامل مع معلومات مالية تجارية واقتصادية أم شخصية[٢].

ب. **العدوان على المعلومات المخزنة بالنظام المعلوماتي:** تقع صورة الإتلاف المعلوماتي بتدمير وإتلاف وتخريب المعلومات المخزنة بالنظام المعلوماتي، ويتحقق ذلك بتدمير وإتلاف وتخريب المعلومات المخزنة بالنظام المعلوماتي بحيث تصبح بلا معنى ولا يمكن الاستفادة منها، وهو لا يسري على النظام المعلوماتي ككل، وعلى التعاملات الإلكترونية[٣].

ج. **تضخيم البريد الإلكتروني:** أن يتم إرسال نسخ مكررة بعدد كبير من الرسائل، بما يترتب عليه إعاقة سير النظام التقني المعلوماتي بشكل من ضبط، ويؤدي ذلك الأمر إلى إعاقة استخدام تلك الخدمة أو توقفها وفي الغالب يتم هذا الأمر من خلال فيروسات معلوماتية يتم بثها ونشرها عن طريق الإنترنت[٤].

د. **الاعتداء عن طريق وسائل الإتلاف المعلوماتي:** حيث تُعد فيروسات الحاسب الآلي برمجيات مشفرة لإتلاف الحاسب الآلي مثل أي برمجيات أخرى يتم تصميمها بهدف محدد وهو إحداث أكبر ضرر ممكن بأنظمة الحاسب الآلي، وتتميز بقدرتها على ربط نفسها بالبرامج الأخرى وإعادة إنشاء نفسها حتى تبدو وكأنها تتكاثر وتتوالد ذاتيًا، بالإضافة إلى

---

(١) د. ماجد عمار، المسئولية القانونية الناشئة عن استخدام فيروس برامج الكمبيوتر ووسائل حمايتها، دار النهضة العربية، القاهرة، ١٩٨٩م، ص٣٥.

(٢) د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، ٢٠٠١م، ص١٣١.

(٣) د. عبد الحق حميش، حماية المستهلك الإلكتروني، بحث مُقدم إلى مؤتمر الأعمال المصرفية بين الشريعة والقانون، كلية الشريعة والقانون وغرفة تجارة وصناعة دبي، الإمارات العربية المتحدة، ١٠-١٢ مايو ٢٠٠٣، ص١٢٦٧.

(٤) د. عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، "الأحكام الموضوعية والأحكام الإجرائية"، دار النهضة العربية – القاهرة، ٢٠١٤م، ص٣٥١.

قدرتها على الانتشار من نظام إلى آخر عبر شبكات الاتصال العالمية أو بواسطة قرص ممغنط [١].

وما تجب الإشارة إليه أن استعمال لفظ الفيروس هو مجازاً، فهو في الحقيقة برنامج للحاسب الآلي، وهو ليس فيروساً بالمعنى العضوي أو البيولوجي، بالرغم من أنهما يشتركان في بعض الخصائص [٢].

١. **القدرة على التخفي:** المقصود بالتخفي هنا: هو أنه غالباً ما قد يتخفى داخل أحد البرامج العادية التي يقوم المستخدم بتحميلها من الإنترنت معتقداً سلامة هذه البرامج وخلوها من أي أضرار.

٢. **الانتشار:** إن سرعة الانتقال من نهاية طرفيه إلى باقي الأطراف الداخلة في الشبكة في ثوان معدودة بسبب التكاثر اللانهائي، وقد ساعد على هذا الانتشار التوافق في البرامج المستخدمة على نطاق واسع عبر دول العالم، وشبكات المعلومات (الإنترنت)، وعلاوة على ما سبق، يأتي الانتشار مكملاً للتخفي، فبعد قيام المستخدم بتحميل البرنامج الذي يحوي فيروساً ويثبته في جهازه، يبدأ الفيروس بالانتشار والتوسع داخل الجهاز تمهيداً لقيامه بالغرض المعد لأجله سواء كان إتلاف البرامج الموجودة داخل الجهاز جزئياً أو كلياً[٣].

٣. **الاختراق:** للفيروس القدرة كذلك على اختراق البرامج المثبتة على الحاسب الآلي وإتلافها والتي قد يكون من ضمنها البرامج المضادة للفيروسات، وهي الوظيفة التي أعد من أجلها الفيروس.

٤. **القدرة على العدوى:** فالفيروس لا يصيب جهاز الشخص المجني عليه فحسب. بل قد ينتقل عبر شبكة الإنترنت إلى غيره من الأجهزة، كما يعد فيروس الحاسب الآلي عبارة عن برنامج يتم تسجيله أو زرعه على الأقراص أو الأسطوانات الخاصة بالحاسب الآلي، ويظل خاملاً لفترة محددة، ثم ينشط فجأة في توقيت معين ليدمر البرنامج أو المعلومات المخزنة أو يتلفها جزئياً وذلك بالخرق أو التعديل، ومن هنا يُعتبر الفيروس شديد الصلة بالجريمة، فهو أداة لارتكابها حيث يؤدي إلى تعطيل أو إفساد نظام المعالجة الآلية، أو إلى محو وتعديل البيانات. فضلاً عن قدرة الفيروس على النسخ الآلي والذاتي والتلقائي، فهو عبارة عن برنامج أو مجموعة تعليمات وأوامر للحاسب الآلي تلحق الضرر بنظام المعلومات أو البيانات، وتكون له القدرة على التضاعف والانتشار بأن يقوم عند تشغيله بزرع نسخ منه في الأقراص الصلبة، فهو ينسخ نفسه

---

(١) مقال بعنوان، "جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت". متاح على الرابط التالي: https://www.startimes.com/?t=16193884

(٢) د. محمد حسين منصور، المسؤولية الإلكترونية، منشأة المعارف، الإسكندرية، ٢٠٠٦م، ص٢٩٢.

(3) Arabian Computer News, Vol. 61. Mar. 1989. PP. 10-11.

عدة مرات وينتشر عبر خطوط التوصيلات الإلكترونية، ويصدر معلومات غير صحيحة ويؤدي في النهاية إلى تدمير النظام، وإتلاف البيانات والمعلومات [١].

٥. **القدرة على التدمير:** إن تدمير وتخريب المعلومات والبرامج هو الهدف الأساسي للفيروس المعلوماتي بما يؤدي في النهاية إلى تعطيل أو توقف النظم المعلوماتية، فإن الفيروس يتجه إلى مكان ما في الذاكرة ويظل كامناً[٢]، حتى يتحقق الأمر أو الزمن الذي يعتمد برمجة المفجر في الفيروس عليها، ثم ما يلبث أن يقوم بنشاطه في تدمير المعلومات[٣].

وتتنوع البرامج المستخدمة في جريمة الإتلاف والتدمير المعلوماتي إلى ما يلي:

١. **برامج الدودة:** وهي عبارة عن برامج تقوم باستغلال أي فجوة في أنظمة التشغيل لكي تنتقل من جانب لآخر أو من أي شبكة إلى أخرى عبر الوصلات التي ترتبط بها، وذلك دون الحاجة إلى تدخل إنساني لتشغيلها، وهذا هو الاختلاف بينها وبين حصان طروادة الذي دائماً ما يعتمد على التدخل الإنساني لمباشرة نشاطه، وقد ظهرت هذه النوعية من البرامج الضارة لأول مرة عام ١٩٨٨م، على يد الطالب الأمريكي (موريس) وقد عرفت بعد بدودة موريس[٤].

٢. **حصان طروادة[٥]:** وهو نوع من البرامج الضارة يتخفى غالباً في صورة برنامج شرعي. يمكن أن يستخدم المجرمون الإلكترونيون والمتطفلون أحصنة طروادة في محاولتهم للوصول إلى أنظمة المستخدمين. ينخدع المستخدمون عادةً ببعض أشكال الهندسة الاجتماعية لتحميل أحصنة طروادة وتطبيقها على أنظمتهم، وتسمح أحصنة طروادة بمجرد تنشيطها للمجرمين الإلكترونيين بالتجسس عليك وسرقة بياناتك الحساسة والتسلل إلى نظامك. وقد تتضمن هذه الإجراءات: حذف البيانات–حظر البيانات–تعديل البيانات–نسخ البيانات–تعطيل أداء الحواسيب أو شبكات الحواسيب–وذلك على خلاف فيروسات الحاسوب والفيروسات المتنقلة، إذ لا تستطيع أحصنة طروادة التكاثر ذاتياً، فهو عبارة عن برنامج فيروسي لديه القدرة على الاختفاء داخل

---

(١) د. هدى حامد قشقوش، مرجع سابق، ص١٣.

(٢) د. هدى حامد قشقوش، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي في الفترة ٢٥–٢٨ أكتوبر ١٩٩٣ ص٤١٣؛ د. هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، ٢٠٠٠م، ص٤٨، ٤٩.

(3) David Febrache, Pathology of computer viruses, Springs Overlay, New York, 1992, P.30.

(٤) د. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، التحكم في جرائم الحاسب وردعها، دار النهضة العربية، القاهرة، ٢٠٠٥م، ص٣٦٧.

(٥) مقال على الإنترنت: ما فيروس حصان طروادة، "تهديدات أمن الإنترنت".
متاح على الرابط التالي:
https://me.kaspersky.com/resource-center/threats/trojans

برامج أخرى أصلية للمستخدم، وتُعتبر من برامج الاختراق من أجل جمع البيانات والمعلومات، وهو لا يتكاثر ولا يلتصق بالملفات وإنما هو برنامج مستقل بذاته يحمل في طياته توقيت وأسلوب استيقاظه، ولا بد من تدخل الإنسان لتنشيطه.

٣. **القنبلة المعلوماتية:** وهي نوع من البرامج الخبيثة صغيرة الحجم يتم إدخالها بطرق غير مشروعة وخفية مع برامج أخرى، ويؤدي اجتماعها هذا إلى انعدام القدرة على تشغيل برامج الحاسب الآلي، ومن الأمثلة على هذا الفيروس زرع القنبلة المنطقية لتعمل لدى إضافة سجل موظف بحيث تتفجر لتمحو سجلات الموظفين الموجودة أصلًا في المنشأة مثلما حصل في ولاية لوس أنجلوس الأميركية عندما تمكن أحد الأشخاص من وضع قنبلة منطقية، مما أدى إلى تخريب النظام عدة مرات(١).

٤. **القنبلة المنطقية:** هذا النوع ينشط بمجرد حدوث واقعة معينة مثل بدأ تشغيل الجهاز أو عند إنجاز أمر معين في الحاسب الآلي أو عند بدأ تشغيل برنامج معين(٢).

٥. **القنبلة الزمنية:** حيث ينشط الفيروس في تاريخ معين محدد بالذات فهو يثير حدثًا في لحظة زمنية محددة بالساعة واليوم والسنة والوقت اللازم ومثال هذا الفيروس ما قام به شخص يعمل بوظيفة محاسب حيث وضع قنبلة زمنية في شبكة المعلومات الخاصة بالمنشأة بدافع الانتقام، وانفجرت القنبلة بعد مضي ستة أشهر من رحيله عن المنشأة وترتب على ذلك إتلاف كل البيانات المتعلقة بها(٣).

٦. **الباب الخلفي:the back door:** وقد نشأت **برامج** الباب الخلفي في الأصل كآنية يستخدمها المبرمجون لتضمن لهم مدخلًا خاصًا للأنظمة التي يقومون ببرمجتها، خاصة عندما يتسبب خطأ برمجي في التوقف التام للنظام، وفي بعض الأحيان يقومون بذلك لأسباب مشبوهة، ومع الوقت أصبحت تستخدم للولوج إلى الأنظمة الإلكترونية واختراقها والتلاعب بمحتوياتها(٤)، وأنواع شفرة الباب الخلفي كثيرة ومتعددة، لكنها تجتمع في كونها تعطي ولوجًا خاصًا يتجاوز الإجراءات العادية، **ورغم** أن البعض يخلط بينها وبين حصان طروادة إلا أنه يمكن التفريق

---

(١) مقال على الإنترنت: جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت، مرجع سابق، متاح على الرابط التالي: https://www.startimes.com/?t=16193884

(٢) محمد أمين الشوابكة، المرجع السابق، ص٢٤٠.

(٣) انظر في ذلك: مقال بعنوان، "الجريمة المعلوماتية الهادئة"، متاح على الرابط التالي: https://alhwar.com/2019/10/30/%D8%A7

(٤) د. يوسف بن سعيد بن محمد الكلباني، المرجع السابق، ص١٤٨، ١٤٨.

بينهما من حيث أن الأخير يوحي للمستخدم بأنه ذو منفعة، في حين أن برامج الحاسب الخفي تقوم بعملها في الخفاء[١].

٧. **برمجيات ويب التفاعلية:** قد يسئ بعض المبرمجين توظيف بعض البرمجيات المخصصة لمواقع الشبكة المعلوماتية والتي تكون عبارة عن ملفات تنفيذية يتم تحميلها وتشغيلها على جهاز المستخدم فور اتصاله بالموقع الموجودة عليه، ومن هذه البرمجيات برمجيات«**جافا وأكتف أكس**»، ورغم أن هاتين الوسيلتين صممتا بهدف تسهيل تفاعل زوار مواقع الشبكة المعلوماتية إلا أنه متى ما تم برمجتها عن قصد بأعمال أخرى يمكنها أن تلحق بأجهزتهم الكثير من الأضرار[٢].

من جماع ما سبق يتضح جلياً أن المشرع المصري كان موفقًا في الصياغة التشريعية أكثر من المشرع العُماني والتشريعات المقارنة عندما أفرد نصاً خاصاً لجريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة تضمنته المادة ٢٠ من القانون رقم ١٧٥ لسنة ٢٠١٨م بخلاف المشرع العُماني والتشريعات المقارنة التي نصت عليها بين ثنايا كعدة صور تضمنتها قوانين مكافحة جرائم تقنية المعلومات.

---

(١) محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت، دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية، رسالة ماجستير، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، ٢٠٠٤م، ص٣٩؛ ص٤١.

(٢) د. يوسف بن سعيد بن محمد الكلباني، المرجع السابق، ص١٤٩.

المطلب الثاني

العلة من تجريم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة

تمهيد وتقسيم:

إذا كانت الجريمة المعلوماتية تتمثل في غش المعلوماتية، أي كل سلوك غير مشروع يتعلق بالمعلومات المعالجة نقلها؛ فإن محل الجريمة المعلوماتية يتصور من زاويتين، الزاوية الأولى إذا كانت المعلومات هي التي ينفذ بها الاعتداء، فتكون المعلوماتية أداة، حيث إن الجاني يستخدم التقنية المعلوماتية في تنفيذ جرائمه الإلكترونية سواء أكانت الجريمة موجهة ضد الأشخاص أو الأموال أو الدولة[١]. أما الزاوية الثانية فهي محل الاعتداء حيث يتجه قصد الجاني الجرمي إلى الاعتداء على الشيء أو المال المعلوماتي ذاته، فهذا الشيء أو المال المعلوماتي هنا قد يكون الحاسوب بجميع مكوناته المادية والمعنوية أو الشبكات أو البرامج أو المعطيات[٢]. وبالتالي يتعين الأمر الوقوف على فلسفة المشرع الجنائي من تجريم الجريمة محل البحث، وذلك من خلال التقسيم التالي:

الفرع الأول

العبرة في إسباغ الحماية الجنائية للأنظمة المعلوماتية الخاصة بالدولة

من المسلم به أنه دخلت مختلف القطاعات الحكومية إلى عالم المعلوماتية خاصة بعد ظهور الإنترنت، نظراً للخدمات الكبيرة التي تقدمها، باعتبارها تضمن السرعة، وتقليص الوقت والتكاليف، إلا إنه بالمقابل أصبحت عرضة لكي تكون ضحية من ضحايا الجريمة المعلوماتية، ولم تقتصر حدود ثورة المعلومات على القطاع المدني. بل كان لها أكبر الأهمية في تطوير أنظمة الحرب الحديثة، وأدت إلى ظهور ما يُسمى بحرب المعلومات، حيث يستهدف هذا النوع من الإجرام الأهداف العسكرية والسياسية[٣]. فقد أصبحت المعلومات–من خلال هذه الحروب– هي السلاح الرئيس، وبالتالي أدى ذلك إلى تطوير صياغة التنظيمات الهجومية والدفاعية لحرب المعلومات مما يجعل منظومة القوات المسلحة في الحروب المستقبلية والدفاعية لحرب المعلومات مما يجعل منظومة القوات المسلحة في الحروب المستقبلية والدفاعية لحرب المعلومات. حيث تعتمد آليات هذه الحرب على شبكات الحاسب

---

(١)د. علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونياً، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات، دولة الإمارات، ١–٣ مايو ٢٠٠٠، المجلد الثالث ص٥٦١.

(٢) د. نور سليمان يوسف يعقوب البالول، المرجع نفسه، ص١٨.

(٣) صغير يوسف، الجريمة المرتكبة عبر الإنترنت، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري بتيزي وزو، الجزائر، ٢٠١٣م، ص٢٤، ٢٥.

الآلي في نقل المعلومات عن طريق الشبكات، ومن خلال الأقمار الصناعية، حيث يؤدي ذلك بدوره إلى تعاظم دور القوات المسلحة ونظم المعلومات في أنظمة التسليح نظرا لحتمية وأهمية تخزين البيانات وسرعة معالجتها وعرضها بصورة مناسبة أمام القادة لاتخاذ القرار على أساس أهمية تلك المعلومات(١).

وإذا كان المشرع الدستوري قد اعتبر المعلومات والبيانات والإحصاءات والوثائق الرسمية ملك للشعب(٢)، والإفصاح عنها من مصادرها المختلفة، حق تكفله الدولة لكل مواطن، كما ألزم الدولة بتوفيرها وإتاحتها للمواطنين بشفافية، وينظم القانون ضوابط الحصول عليها وإتاحتها وسريتها، وقواعد إيداعها وحفظها، والتظلم من رفض إعطائها، كما يحدد عقوبة حجب المعلومات أو إعطاء معلومات مغلوطة عمداً، وتلتزم مؤسسات الدولة بإيداع الوثائق الرسمية بعد الانتهاء من فترة العمل بها بدار الوثائق القومية، وحمايتها وتأمينها من الضياع أو التلف، وترميمها ورقمنتها، بجميع الوسائل والأدوات الحديثة، وفقًا للقانون(٣).

ومقتضى هذا التفويض الدستوري للمُشرع العادي أن يكون الأصل إباحة المعلومات والبيانات الحكومية الرسمية على شبكة المعلومات الدولية، والاستثناء يكون تقرير سريتها من خلال قانون محدد واضح، لذلك جاء قانون جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨م لكي يرصد حماية جنائية لمواقع وأنظمة الدولة المعلوماتية، وبريدها الإلكتروني، وحساباتها الخاصة وكذا بياناتها ومعلوماتها الحكومية عبر شبكة الإنترنت فحظر دخولها بطريق العمد أو بطريق الخطأ أو اختراقها.

ولا شك أن مسلك المشرع العادي في رصد عقاب جنائي على دخول المواقع والحسابات الحكومية الخاصة للدولة، وبريدها الإليكتروني ينسجم مع ما جاء به الدستور. إذ من حق الدولة كالشخص العادي ألا يدخل أحد على مواقعها وبريدها وحساباتها طالما كانت خاصة، وليس عامة متاحة للجميع، ولكن يثور التساؤل حينما يتعلق الأمر ببيانات ومعلومات الدولة إذ هذه البيانات والمعلومات بنص الدستور ملك للشعب ومن حق المواطنين الحصول عليها ولا تُحجب عنهم إلا بمقتضى قانون ينظم سريتها، ومن ثم؛ فإن ما جاءت به المادة ٢٠ من قانون جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨م من إطلاق الحماية الجنائية على المعلومات والبيانات الحكومية على شبكة الإنترنت، وحظر الحصول عليها دون قصر الحظر على البيانات والمعلومات الإلكترونية الحكومية السرية فيه نظر من الناحية القانونية، حيث إن قانون تقنية المعلومات المصري لم يضع تعريفًا أو

---

(١) أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دار النهضة العربية، القاهرة، ٢٠٠٥م، ص٤٢.

(٢) المادة ١٩ من العهد الدولي الخاص بالحقوق المدنية والسياسية لسنة ١٩٦٦م.

(٣) المادة ٦٨ من دستور جمهورية مصر العربية الصادر في عام ٢٠١٤م والمعدل في ٢٠١٩م.

تحديداً للبيانات السرية؛ الأمر الذي يتعين معه الرجوع إلى قانون العقوبات الذي يبين مفهوم المعلومات والبيانات السرية، وهذه الجريمة من جرائم السلوك المتعدد الذي يتخذ محلها تارة مواقع أو حسابات خاصة أو بريد إلكتروني يُدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوك لها أو يخصها.

كما يتخذ تارة أخرى صورة البيانات والمعلومات الإلكترونية الحكومية، وهي في الصورة الأولى جنحة عقوبتها الحبس لمدة لا تقل عن سنتين، وفي الثانية جناية عقوبتها السجن، وهي من جرائم السلوك المادي ذو المضمون النفسي المتمثل في أن دخول الموقع أو الحساب أو البريد عمداً أو بإهمال أو تجاوز حدود الحق المخول بالدخول أو اخترق الموقع أو البريد أو الحساب.

والعبرة في إسباغ الحماية الجنائية المقررة للمواقع الإلكترونية أو الحسابات الخاصة أو البريد الإلكتروني يكون بنعتها بالصفة الرسمية عليها، وهو ما لا يتحقق إلا بوجود رابطة بينها وبين الدولة، وهذه الرابطة هي أن هذا الموقع أو الحساب الخاص يُدار بمعرفة الدولة أو أحد الأشخاص الاعتبارية العامة أو لحساب الدولة أو أحد أشخاصها الاعتبارية، أو كان مملوكًا للدولة أو أحد أشخاصها الاعتبارية أو يخصهما، ومن ثم يكون الحساب أو الموقع رسمياً إذا كان خاضعًا لإدارة الدولة أو مملوكًا لها[1]، ويُقصد بالدولة الحكومة وأجهزتها ووحدات الحكم المحلي، بينما يقصد بالأشخاص الاعتبارية العامة الهيئات والمؤسسات العامة وغيرها من الجهات التي يقرر لها القانون الشخصية الاعتبارية العامة. **أما البيانات الحكومية:** فهي بيانات متعلقة بالدولة أو أحد سلطاتها، وأجهزتها أو وحداتها، أو الهيئات العامة، أو الهيئات المستقلة والأجهزة الرقابية، وغيرها من الأشخاص الاعتبارية العامة وما في حكمها، والمتاحة على الشبكة المعلوماتية أو على أي نظام معلوماتي أو على حاسب أو ما في حكمها[2].

ولقد انتهج المشرع المصري في قانون مكافحة جرائم تقنية المعلومات حماية لأسرار الدولة للبيانات والمعلومات الإلكترونية المتعلقة بالدولة أو أحد سلطاتها أو أجهزتها أو وحداتها أو الهيئات العامة أو الهيئات المستقلة أو الأجهزة الرقابية أو هيئاتها العامة الخدمية أو الاقتصادية، وغيرها من الأشخاص الاعتبارية العامة أو ما في حكمها المتاحة على الشبكة المعلوماتية أو أي نظام معلوماتي أو حاسب خاص بها. لذلك استلزم المشرع المصري أن يكون محل جريمة الاعتداء على الأنظمة

---

(١) د. رامي متولي القاضي، المواجهة الجنائية لجرائم تقنية المعلومات في التشريع المصري في ضوء أحكام القانون ١٧٥ لسنة ٢٠١٨م، مقارناً بالمواثيق الدولية والتشريعات المقارنة، مجلة البحوث القانونية والاقتصادية، العدد ٧٥، كلية الحقوق، جامعة المنصورة، مارس ٢٠٢١م، ص١٠٦٦.

(٢) قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨م؛ قانون مكافحة جرائم تقنية المعلومات العماني؛ المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم الإلكترونية الإماراتي.

المعلوماتية الخاصة بالدولة موقعًا أو بريدًا إلكترونيًا أو حسابًا خاصًا أو نظامًا معلوماتيًا يُدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوك لها أو يخصها، وتبرز الإشارة إلى أن المواقع الحكومية هي المواقع التابعة للنطاق الإلكتروني الخاص بالدولة، وغالبًا ما ينتهي عنوانها بـ gov[1]، اختصاراً لكلمة government، وقد تم تخصيص هذا النطاق للدوائر والمؤسسات الحكومية تمييزاً لها عن غيرها.

وحدد المشرع البيانات والمعلومات الإلكترونية بأنها كل ما يمكن إنشاؤه أو تخزينه، أو معالجته، أو تخليقه، أو نقله، أو مشاركته، أو نسخه بواسطة تقنية المعلومات؛ كالأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور والأصوات وما في حكمها، وأن البرنامج المعلوماتي عبارة عن مجموعة الأوامر والتعليمات المعبر عنها بأية لغة أو رمز أو إشارة، والتي تتخذ أي شكل من الأشكال، ويمكن استخدامها بطريق مباشر أو غير مباشر في حاسب آلي لأداء وظيفة أو تحقيق نتيجة سواء كانت هذه الأوامر والتعليمات في شكلها الأصلي أو في أي شكل آخر تظهر فيه من خلال حاسب آلي، أو نظام معلوماتي.

ويُلاحظ أنه إذا ما كان التجريم هو أقصى مراتب الحماية التي يضفيها التشريع على نوع معين من المصالح المهمة للمجتمع، فإن النص الجنائي وبحكم طبيعته القانونية، يستجيب لكل متغير اجتماعي معين يطرأ على المجتمع، لذلك كانت ظاهرة الحاسب الآلي ومفاعيله، وما أفرزته من ظواهر ورتبته من آثار، محط اهتمام النشاط التشريعي الجنائي لحماية المصالح الاجتماعية التي أفرزتها هذه المنظومة التقنية [2].

والمصلحة القانونية هي أحد الأفكار التي كشفت عنها نظرية القيم، التي قادت إلى التصور الاجتماعي للقانون، وأبرزت التلازم الحتمي بين القانون والمجتمع، فهي حكمة التجريم، وهي المعيار الذي يستعين به المشرع في مرحلة الصياغة والتطبيق وفي تفسير غائي للقاعدة القانونية يربط بينها وبين متطلبات الحياة [3]، والقانون بوصفة أداة تنظيم المجتمع، هو المنوط به تنظيم العلاقات المختلفة التي تتحول بمقتضى هذا التنظيم إلى مصالح قانونية، تعبر عن القيم التي تسود الجماعة، وقانون العقوبات يتولى حماية عدد من المصالح القانونية، عن طريق التهديد بالعقاب، ومن هنا فإن المصلحة

---

(١) د. رامي متولي القاضي، المرجع السابق، ص١٠٦٥.

(٢) د. محمود عبد الرحيم الديب، الحماية القانونية للملكية الفكرية في مجال الحاسب الآلي والإنترنت، دار الجامعة الجديدة للنشر والتوزيع، الإسكندرية، ٢٠٠٥م، ص٥٩.

(٣) د. مأمون محمد سلامة، النظرية الغائية في السلوك الجنائي، بحث منشور في المجلة الجنائية القومية، القاهرة، المجلد الثاني عشر، العدد الأول، ١٩٦٩م، ص ١٥٤.

الاجتماعية، وما تعبر عنه من قيمة اجتماعية هي الموضوع القانوني للجريمة، وهو ما يبرز أهمية مضمون القاعدة الجنائية وما ابتغاه المشرع منها، لدراستها دراسة موضوعية[١].

فالمصلحة المحمية في جرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة هي القاعدة التي يستعين بها المشرع في مرحلتي التقنين والتطبيق؛ كمعيار في هذه العملية، والمصلحة المحمية هي إحدى قيم الجماعة التي تكسب الواقعة المادية مدلولها الاجتماعي، كما أن المصلحة المحمية هي حكمة التجريم، وهي تمثل تفسير القاعدة القانونية وعلاقتها بمقتضيات الحياة، كما تُعد المصلحة صورة من صور الحماية القانونية التي يُقصد بها حماية المصالح الأساسية للأشخاص، والمصلحة العامة في الاستقرار، وضمان أمن المجتمع، وممارسة حقوقه[٢].

وعندما يرغب المشرع في كفالة الحماية الجنائية لمصلحة اجتماعية معينة؛ فإنه يلتزم بتحري أهداف النظام القانوني الكلي، والحقوق واللتزامات والمصالح القانونية المقررة في فروعه الأخرى. واضعا نصب عينيه، الخلق والشعور العام، والمبادئ والقيم العليا الاجتماعية، ودرجة الشعور الديني في المجتمع، وما يدعم هذا المجتمع من عادات وتقاليد وعرف، ومعايير العدالة السائدة [٣]، مستفيداً من نتائج العلوم المساعدة لقانون العقوبات [٤] مستهدياً بالتجارب التشريعية المقارنة عبر التاريخ، سواء من حيث تحديد مصادر العدوان، أو صوره وأشكاله، أو أسلوب وخطة الحماية للمصالح المشابهة لتلك التي يعمل على صياغة قاعدة تكفل حمايتها. كما أن هذه الحماية في إطار التوازن مع المصلحة العامة المتمثلة في النظام العام لجميع جوانبه بحيث تتطلب تنظيم ممارسة هذه الحقوق والحريات داخل حدود معينة مراعاة للصالح العام، وتجريم أي خروج عن هذه الحدود، وهو ما يمثل الضرورة الاجتماعية التي تتطلب التجريم والعقاب مع الفعل الصاد الذي تتطلبه، من كل ما تقدم نصل إلى أن المصلحة المحمية في هذه الجرائم –محل الدراسة –هي التي توصلنا إلى تحديد الأفعال الماسة بأمن الدولة ونظامها المعلوماتي، ومن ثم؛ التصدي لها من خلال تجريمها والمعاقبة عليها[٥].

ولا شك أن المصالح المُراد حمايتها في هذه الجرائم، هي مصالح عامة، بمعنى أن المصالح العامة هي التي يهدف المشرع حمايتها من التعرض للخطر، وهذه الحماية تتطلب من المشرع تجريم كل نشاط خطر من شأنه تعريض هذه المصالح للخطر، وأن المصلحة المحمية هي سبب وجود الترابط

---

(١) د. مأمون محمد سلامة، جرائم الموظفين ضد الإدارة العامة في ضوء المنهج الغائي، بحث منشور في مجلة القانون والاقتصاد، كلية الحقوق، جامعة القاهرة، المجلد ٣٩، العدد الأول، مارس ١٩٦٩م، ص٢.

(٢) عباس منعم صالح، الحماية الجنائية لأمن الدولة الداخلي، رسالة ماجستير، كلية القانون، الجامعة المستنصرية، العراق، ٢٠١٢م، ص٦٩.

(٣) د. عبد الرزاق السنهوري و د. أحمد حشمت أبو ستيت، أصول القانون، دار النهضة العربية، القاهرة، ١٩٩٢م، ص ٢٢٠.

(٤) د. أحمد سلامة، النظرية العامة للقانون، مطبعة الاستقلال، ١٩٧١م، ص ٧٤ وما بعدها.

(٥) في ذلك المعنى: عباس منعم صالح، المرجع السابق، ص٧٢.

بين القواعد القانونية الجديرة بالحماية والمجتمع، وهذا ما كشفته نظرية القيم عن التصور الاجتماعي للقانون، والمصلحة كذلك هي حكمة التجريم وهي المعيار الذي يستند عليه المشرع في تشريع القوانين وتطبيقها، كما أن المصلحة تعد من أحد قيم الجماعة التي تكسب الواقعة المادية مدلولها الاجتماعي، والقانون بشكل عام ينظم العلاقات بين الإفراد والمجتمع، وذلك باعتباره أداه تنظيم المجتمع، وهذه العلاقات هي المصالح الأساسية التي يعد القانون بشكل أساسي لحمايتها ويعدها تعبير عن قيم المجتمع(١).

وينبغي أن تكون هذه المصلحة ذات قيمة اجتماعية(٢) وتتدرج صور الجزاء من حيث جسامتها تبعاً لأهمية المصالح محل الحماية، ويتكفل القانون الجنائي بإسباغ صفة التجريم ثم تقرير العقاب على كل سلوك ينطوي على عدوان يلحق بالمصالح ذات المكانة العليا في نظر المشرع(٣).

لذلك حظر المشرع الاعتراض أو الاختراق للبيانات والمعلومات الحكومية على شبكة الإنترنت حماية للأمن القومي، وأن حماية أسرار الدولة للبيانات والمعلومات الإلكترونية وأجهزتها على الشبكة المعلوماتية أو نظام معلوماتي أو حاسب خاص من مسائل الأمن القومي، والأمن القومي يتسع، ولا يضيق ليشمل كل ما يتصل باستقلال واستقرار وأمن الوطن ووحدته وسلامة أراضيه، وأن الأمن المالي والاقتصادي للوطن جزء لا يتجزأ من أمنه القومي، وأن الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة جريمة لها عقوبات متعددة صارمة.

ومن أسباب تشديد العقوبة أن المساس في هذه الجرائم واقع على شخصية الدولة وكيانها، فهي المحل الأساسي الذي ينصب عليه الاعتداء في الجرائم الواقعة على أمن الدولة التي تقترف ضد الدولة وتهدف إلى إضاعة استقلالها، أو الانتقاص من سيادتها، أو تهديد سلامة أراضيها، وتنال الوطن في كيانه ووجوده والسعي الى هدم هذا الكيان أو الجرائم التي ترتكب ضد الدولة وتهدف إلى الانقضاض على أجهزة الحكم، أو مؤسساتها أو مواطنيها، وتطال الحكومة في مساسها (٤).

ولا شك أن للأمن دور في الحفاظ على أمن وأراضي ومواطني ومكتسبات ومقدرات ومصالح الوطن في عالم تتزايد فيه أشكال مهددات الأمن الوطني، وما يستدعيه ذلك من استعداد في سرعة التجاوب ودقة في التنفيذ للتصدي للمخاطر الأمنية في اتجاهات متسقة ومسارات متزامنة لذلك، كما أنه عندما تتعلق المعلومات والبيانات بالأمن الوطني فإنه يجب تصنيفها لخطورتها من جانب ولتوفير أكبر

---

(١) د. مأمون محمد سلامة، جرائم الموظفين ضد الإدارة العامة، المرجع السابق، ص١٢ وما بعدها.

(٢) د. فتحي عبد الرحيم عبد الله، مقدمة العلوم القانونية، الكتاب الثاني، نظرية الحق، ١٩٩٩م/٢٠٠٠م، ص٢٧.

(٣) د. حسنين إبراهيم صالح عبيد، فكرة المصلحة في قانون العقوبات، بحث منشور بالمجلة الجنائية القومية، القاهرة، العدد الثاني، ١٩٦٩م، ص٢٥٧ وما بعدها.

(٤) د. نور سليمان يوسف يعقوب البالول، المرجع نفسه، ص٣٥٥.

قدر من الحماية الجنائية لها من جانب آخر، فمصطلح الأمن الوطني يشير إلى كل شيء يتعلق بسلامة الدولة ضد الأخطار الخارجية والداخلية التي قد تؤدي بها إلى الوقوع.

وما تجب الإشارة إليه أنه يتجه البعض إلى أن العدوان على الصفحات الرسمية الحكومية على مواقع التواصل الاجتماعي يبقى خارج نطاق التجريم، حيث إن هذه الصفحات وإن كانت حكومية إلا أنها منشأة على مواقع إلكترونية غير حكومية، بالنظر إلى أن مواقع التواصل الاجتماعي هي مواقع خاصة مملوكة لشركات خاصة، ولا يمكن أن ينسحب وصف المواقع الإلكترونية الحكومية على تلك الصفحات(١).

ولكن يُلاحظ أنه وإن كان الاتجاه آنف الذكر صحيحاً، إلا أن النص القانوني الوارد بالمادة (٢٠) من قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨م يتسع ليشمل الحسابات الخاصة للدولة على مواقع التواصل الاجتماعي، حيث إن نص المادة آنفة الذكر يشير إلى تقرير الحماية الجنائية لأي موقع أو بريد إلكتروني أو حساب خاص أو نظام معلوماتي يدار بمعرفة الدولة أو لحسابها أو أحد الأشخاص الاعتبارية العامة أو مملوك لها أو يخصها، وما يؤيد الاتجاه الأخير حقًا أن الدول في الوقت الراهن قد أصبح لديها حسابات خاصة على مواقع التواصل الاجتماعي، الأمر الذي يتعين معه أن تكون تلك الحسابات خاضعة للتجريم من أي اعتداء قد يقع عليها.

الفرع الثاني

المصالح المحمية من تجريم الاعتداء على الأنظمة المعلوماتية للدولة

إن من طبيعة أي دولة أن تمتلك الأسرار التي لا ينبغي لأي شخص أن يقوم بالاطلاع عليها دون إذن مسبق، وأي اطلاع عليها أو اعتداء قد يؤدي لحدوث أزمات داخلية وخارجية، إذن فهذا النوع من المعلومات ينم عن خطورة كبيرة، لذلك فقد جاءت التشريعات على حماية البيانات والمعلومات التي تؤثر على أمن الدولة الداخلي(٢) والخارجي، والمحفوظة في النظام المعلوماتي والشبكات والمواقع الإلكترونية (٣).

---

(١) د. رامي متولي القاضي، المرجع السابق، ص١٠٦٦.

(٢) د. إبراهيم محمود اللبيدي، الحماية الجنائية لأمن الدولة، دار الكتب القانونية، مصر، ٢٠١٠م، ص٣٩؛ د .أسامة أحمد المناعسة، الوسيط في شرح قانون محكمة أمن الدولة، الطبعة الأولى، دار الكتاب الحديث، القاهرة، ٢٠٠٩م، ص١٥.

(٣) د. عبد الإله محمد النوايسة وآخرين، جرائم التجسس الإلكتروني في التشريع الأردني: دراسة تحليلية، مجلة دراسات–علوم الشريعة والقانون، عمادة البحث العلمي، الجامعة الأردنية، المجلد ٤٦، ملحق، ٢٠١٩م، ص٤٦٧.

وتُقسم الأسرار التي يطلع عليها الموظف بحكم طبيعته إلى صور عدة، فهناك من يصنفها إلى أسرار بطبيعتها والأسرار الحكمية، والأسرار بناءً على نص قانوني أو تعليمات إدارية، وثمة من يصنفها إلى: أسرار حكومية، وأسرار إدارية أي متعلقة بالموظفين ذاتهم، فالأسرار الحكومية: هي الأسرار المتصلة بوظيفة الدولة بوصفها حكومة تقوم على السياسة العليا للدولة، كالأسرار العسكرية والأمنية والأسرار المتصلة بعلاقات الدولة بالدول الأخرى، وهذه الأسرار يجب أن تبقى طي الكتمان حرصاً على سلامة الدولة، أما الأسرار المتعلقة بالموظفين ذاتهم، فهي كالظروف الشخصية التي يعلم بها الرئيس أو المسؤول الإداري وبعض الزملاء داخل المؤسسة(١).

وبالتالي فإن قيام الجاني بالدخول أو الولوج إلى النظام المعلوماتي الخاص بالدولة بقصد الاعتداء على بيانات أو معلومات غير متاحة للجمهور، تمس الأمن الوطني، أو العلاقات الخارجية للدولة، أو السلامة العامة، أو الاقتصاد الوطني، من خلال حذفها أو إتلافها، أو تدميرها، أو تعديلها أو تغييرها أو نقلها أو مسحها أو إفشائها يُعد جريمة تنال من أسرار الدولة، واعتداء على حقها في سرية هذه المعلومات، وعدم كشفها(٢)، ولما يؤدي إليه إفشاؤها من مخاطر تهدد أمن الدولة والنظام العام وتسيير المرافق العامة، وقد ينجم عنها أضرار بالغة الخطورة على الدولة والمجتمع لا سيما وإن كانت أسرار تخص الأمن الوطني والدفاع، فضلًا عن تأثيرها على علاقة الثقة بين المواطن والإدارة، ونشر الفوضى، ومن ناحية أخرى وهي التأثير في الثقة بكيان الدولة خارجياً، الأمر الذي يشكل خطراً داهماً على تعاملات الدولة ويعرضها لخسائر كبيرة(٣).

والأمن الوطني اصطلاح يُشير إلى كل شيء يتعلق بسلامة الدولة ضد الأخطار الخارجية والداخلية التي قد تؤدي بها إلى الوقوع تحت سيطرة أجنبية نتيجة ضغط خارجي أو انهيار داخلي، أما العلاقات الخارجية فإنها تشمل كل ما يتعلق بالسياسة الخارجية للدولة، وعلاقة الدولة بالدول الأخرى في شتى المجالات السياسية والاقتصادية والعسكرية، وعلاقتها مع المنظمات الدولية(٤).

وتختلف المصلحة محل الحماية في جرائم أمن الدولة الداخلي عنها في جرائم أمن الدولة الخارجي. ففي الطائفة الأولى فإن المصلحة المحمية هي نظام الحكم ومؤسسات الدولة وبصفة عامة هي حماية الدولة بصفتها شخصاً من أشخاص القانون الداخلي. أما في الطائفة الثانية من الجرائم فالمصلحة المحمية هي وجود الدولة واستقلالها وسلامة أراضيها واحترامها بين الدول أي حماية الدولة

---

(1)Roland Drago et Jean-Marie Auby,"Traité de contentieux administratif",Librairie générale de droit et de jurisprudence impr. R. Vançon , 1962, P.546.

(٢) د. عبد الإله محمد النوايسة وآخرين، المرجع السابق، ص٤٦٧، ٤٦٨.

(٣) د. إبراهيم محمود اللبيدي، المرجع السابق، ص٨٠.

(٤) د. عبد الوهاب الكيالي، موسوعة السياسة، الجزء الأول، الطبعة الأولى، المؤسسة العربية للدراسات والنشر، بيروت، لبنان، ١٩٩٠م، ص٣٣١.

باعتبارها شخصا من أشخاص القانون الدولي[١]. فالغاية في جرائم أمن الدولة الخارجي هي حماية شخصية الدولة في مواجهة الدول الأخرق بالمحافظة على وحدتها واستقلالها وسلامة أراضيها بينما الغاية في أمن الدولة الداخلي هي التجريم لحماية النظام الدستوري أي الحكم ومؤسسات الدولة[٢].

أما السلامة العامة فإنه يُقصد بها السيطرة على ما يُشكل خطراً عاماً أيًا كان مصدره، ومثالها: المعلومات والبيانات التي تتعلق بالمخاطر المحتملة من مفاعل نووي إذا حدث تسريب أو انفجار، والمخاطر الناتجة عن دفن النفايات الخطرة، أو أثر حصول اعتصامات أو مظاهرات على تعريض سلامة المواطنين للخطر، أما الاقتصاد الوطني فيشمل السياسة الاقتصادية الداخلية والخارجية، وكل ما يتعلق بالوضع الاقتصادي والمالي للدولة غير المعلن للجمهور [٣]. إذ تؤثر تلك الجرائم في الاستقرار الاقتصادي للدولة، مما يؤدي إلى طرد الاستثمارات الأجنبية ورؤوس الأموال، حيث يزرع الخوف في نفوس المستثمرين الأجانب من تشغيل أموالهم داخل تلك الدولة التي تنتشر فيها القلاقل والفتن والفوضى والإرهاب[٤].

من جماع ما سبق يتضح أن المصلحة الجديرة بالحماية فيما يتعلق بجرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة–والتي من أجلها أسبغ المشرع صفة التجريم والعقاب على كل سلوك ينطوي على تعريض مصالح الدولة وأمنها ونظامها المعلوماتي للخطر–تتمثل في حماية النظام السياسي للدولة، والحفاظ على وجودها وبقائها، وأمنها، وسلطاتها، وكذلك الحفاظ على الكيان الاجتماعي والاقتصادي للدولة. فقد يكون الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة كما في صورة التجسس الإلكتروني، الذي قد يكون سياسيًا لمعرفة المواقف السياسية لصناع القرار في الدولة والمعلومات التي تتعلق بالسياسة الداخلية والخارجية المتبعة، أو التي تنوي الدولة السير فيها، وقد يكون ذلك معنويًا ونفسيًا لشعوب الدول وقاداتها، ومعرفة مواطن القوة والضعف في شخصية أفراد الشعب، وعوامل الوحدة والتفرقة، والقيم السائدة في المجتمع، التيارات الحزبية والدينية، ومدى تأثيرها في الأزمات، ومقدار العزيمة لدى شعب دولة ما، فالحرب المعنوية من أهم الحروب فمن خلال هذه المعلومات تستطيع الدولة المعادية استخدام السلاح المعنوي، وتحطيم الروح المعنوية للشعب مما يسهل عليها كسب المعركة[٥].

---

(١) د. تامر أحمد عزات، الحماية الجنائية لأمن الدولة الداخلي، دراسة موضوعية إجرائية مقارنة، الطبعة الثانية، دار النهضة العربية، القاهرة، ٢٠٠٧م، ص٦٠.

(٢) د. محمد الفاضل، الجرائم الواقعة على أمن الدولة، الطبعة الرابعة، المطبعة الجديدة، دمشق، سوريا، ١٩٨٧م، ص١٣٥.

(٣) د. عبد الإله محمد النوايسة وآخرين، المرجع السابق، ص٤٦٧، ٤٦٨.

(٤) د. حسنين المحمدي بوادي، إرهاب الإنترنت الخطر القادم، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م، ص٩٧ وما بعدها.

(٥) د. عبد الإله محمد النوايسة وآخرين، المرجع السابق، ص٤٧٠.

كما يوجد هناك ما يُعرف بالتجسس الإلكتروني الاقتصادي، وذلك لمعرفة موارد الدولة وحجم إنتاجها، وميزانها التجاري والاحتياطي لديها، والمدة التي تستطيع خلالها الاعتماد على ذاتها إذا تم حصارها، وكذلك معرفة المرافق الاقتصادية الحيوية لديها، ومواقعها، وكذلكم ديونها الخارجية. كما أن التجسس قد ينصب على المعلومات الصناعية والعلمية من خلال معرفة أسرار الصناعات، والأبحاث العلمية، خاصة إذا كانت هذه الصناعات ترفد الدفاع الوطني فهناك شركات تسهم في الإنتاج الحربي، وتطوير الأسلحة، وقد يكون التجسس العلمي لمعرفة الدراسات العلمية في المجالات الزراعية، أو الهندسية، أو الصحية (١).

ولقد استغلت الجماعات الإرهابية المتطرفة مؤخراً الطبيعة الاتصالية لشبكة المعلومات الدولية، وذلك من أجل بث معتقداتها وأفكارها، بل تعدى الأمر إلى ممارسات تهدد أمن الدولة المعتدى عليها، خاصة المتمثلة في الإرهاب(٢) والجريمة المنظمة(٣)، اللذان أخذا منحى آخر في استعمال الإنترنت، التي سمحت لهم في ارتكاب جرائم غاية في الفتك في حق المجتمعات والدول، بل الأخطر من ذلك أتاحت الإنترنت للكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالاطلاع على مختلف الأسرار العسكرية والاقتصادية لهذه الأخيرة، خاصة فيما يتعلق بالدول التي يكون بينها نزاعات.

ولخطورة الإرهاب الإلكتروني على الساحة الدولية فقد تمت مناقشته خلال المؤتمر الدولي السابع عشر لقانون العقوبات الذي انعقد في بكين عام ٢٠٠٤م، حيث تناول المؤتمر تقرير عام عن الجريمة الإلكترونية والإرهاب السيبراني، والاستغلال الجنسي للأطفال. كما دعت جمهورية مصر العربية في رئاستها لدورة مجلس الأمن عام ٢٠١٦م شركة مايكروسوفت لاجتماع عاجل لبحث تداعيات ظاهرة الإرهاب الإلكتروني، وكيفية منعها، وقمعها تحت مظلة دولية(٤).

ويبقى المساس بالأمن الفكري من بين أخطر الجرائم المرتكبة عبر الإنترنت، حيث تعطي الإنترنت فرصاً للتأثير على معتقدات وتقاليد مجتمعات بأكملها مما يسهل خلق الفوضى، والتطرف الفكري هو في حقيقته انحراف فكري عن الفكر الوسطي للمجتمع، سواء أكان هذا الانحراف فردياً أم جماعياً، وسواء كان انحرافاً دينياً، أم اجتماعياً أم سياسياً، وهو بهذا لا يقتصر على مكان دون آخر،

---

(١) د. جابر المراغي، جرائم انتهاك أسرار الدفاع عن البلاد من الناحيتين الموضوعية والإجرائية، دار النهضة العربية، القاهرة، ١٩٨٨م، ص١١٦.

(٢) د. عبد الله بن عبد العزيز اليوسف، أساليب تطور البرامج والمناهج التدريبية لمواجهة الجرائم المستحدثة، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ٢٠٠٤م، ص٢٥.

(3)Stephane Debray,"Internet face aux substances illicites",complice de la cybercriminalité ou outil de prévention ?, DESS média électronique & Internet de l'Université de Paris 8, Année académique 2002-2003, P.13.

(4)Security Council Presidential Statement Seeks Counter-Terrorism Committee Proposal for 'International Framework' to Curb Incitement, Recruitment,11 MAY 2016, available at : https://www.un.org/press/en/2016/sc12355.doc.htm The last increase in 19/11/2022.

ولا على قُطر دون قُطر آخر، ولا على مذهب ديني، أو فكر سياسي معين، فهو وباء عالمي إنساني، وانحراف يخالف القيم الروحية والأخلاقية والحضارية للمجتمع، ويخالف الضمير المجتمعي، ويخالف المنطق والتفكير السليم، وقد يتخذ الانحراف الفكري صورة الكراهية أو التمييز(١). كما تؤدي جرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة إلى توتر العلاقات بين الدول أحيانًا، وذلك في حال ما إن قامت دول أخرى بإيواء مرتكبي تلك الجرائم خاصة الإرهابيين منهم، ورفض تسليم مرتكبي مثل هذه الجرائم؛ الأمر الذي يؤدي إلى تصاعد الخلافات والتوتر في العلاقات فيما بين الدولتين وخاصة من جانب الدولة التي وقع الاعتداء على رعاياها(٢).

نخلص مما تقدم أن المعلومات الموجودة بالأنظمة المعلوماتية الخاصة بالدولة تكون على شكل محتوى إلكتروني، غير أن المخزن الإلكتروني الموجود فيه تلك الأسرار تكون عرضة للاختراق، أو الحصول على هذه الأسرار وإفشائها، الأمر الذي يتعين معه تجريم كافة صور الاعتداء على هذه الأنظمة حتى لو كان هذا المحتوى محاط بوسائل الأمن المعلوماتي، حتى لا يؤدي ذلك الاعتداء لتعريض مصالح الدولة وأمنها ونظامها المعلوماتي للخطر لا سيما وأن تلك المعلومات قد تكون عسكرية أو سياسية أو اقتصادية، أو أمنية. كما أنه تبلور العلة من تجريم الاعتداء على الأنظمة المعلوماتية والمواقع الإلكترونية الخاصة بالدولة أو الأشخاص المعنوية العامة فيما يلي(٣):

١. مواجهة محاولات الاعتداء على الأنظمة المعلوماتية والمواقع الإلكترونية والحسابات المملوكة للدولة أو أحد الأشخاص الاعتبارية العامة، وتوفير الحماية القانونية لتأمين هذه المواقع أو الحسابات.

٢. تُعد المواقع الحكومية هي المواقع الأكثر رسمية وتمثيلًا لسيادة الدولة على الفضاء الإلكتروني، وأن العدوان عليها يؤثر بشكل كبير في هيبة الدولة وفي نفوس المواطنين.

ولا شك أن الأنظمة المعلوماتية المستخدمة في أي منظمة حكومية تكون مهددة من قبل أشخاص غير مصرح لهم بالدخول لمحاوله تدمير أو سرقة المعلومات أو التغير في المعلومات، أو التجسس، الأمر الذي يتعين معه ضرورة البحث عن إجراءات تساعد في حصر تلك التهديدات.

ومن أهم الإجراءات التي تساعد في حصر تلك التهديدات هي أن تقوم المنظمة بتحديد الأشخاص المخول والمصرح لهم بالدخول، حيث يُشكل العاملين بالأنظمة المعلوماتية الخاصة بالدولة

---

(١) د. عبد الإله محمد النوايسة، دور قانون مكافحة الجرائم الإرهابية الإماراتي في مكافحة الخطورة الإجرامية في جرائم الإرهاب، مجلة جامعة الشارقة للعلوم القانونية، المجلد ١٥، العدد ١، رمضان ١٤٣٩هـ/ يونيو ٢٠١٨م، ص٣٨٣، ٣٨٤.

(2)Francois Debrix,"Tabloid Terror:War, Culture, and Geopolitics",Published by Routledge, London, U.K., 2008, P.22.

(٣) د. رامي متولي القاضي، المرجع السابق، ص١٠٦٥.

في المؤسسات الحكومية أقوى وأخطر أنواع التهديدات لأنه قد يرتكب الشخص خطأ عند استخدامه للنظام يؤدي إلى تقليل فاعلية عمل النظام، كما يمكن أن يقوم بتوظيف شخص ليس لديه كفاءة في العمل على النظام، لذلك وضعت إجراءات لأجل توظيف الشخص المناسب للعمل بتلك الأنظمة، تتمثل فيما يلي[١]:

١. التحري الدقيق للأشخاص الذين تقدموا لأجل الوظيفة الحكومية للعمل على أنظمة الحاسب الآلي التي تحوي معلومات خاصة بالدولة، مع استبعاد الموظفين الذين من شأنهم تخريب العمل وكيفية سيره.

٢. الحرص على توظيف الأشخاص الأكثر كفاءة، وخبرة، وقدره على الإبداع، والعمل في هذا المجال مما يؤدي لتقليل حدوث الأخطاء.

٣. إعطاء الموظفين والعاملين الجدد في النظام المعلوماتي الحكومي دورات تدريبية خاصة مع إخضاع كافة العاملين للمراقبة لأجل ضمان سرية المعلومات والوثائق الخاصة بالدولة.

٤. كتابة تعهد خطي للموظفين بالحفاظ على سرية المعلومات الخاصة بالدولة، وعند انتهاء خدمات هؤلاء الموظفين فإنه يتعين تغيير الكلمات السرية والمعلومات التي من شأنها إدخاله للنظام المعلوماتي الخاص بالدولة.

وتشير التقديرات إلى أن نسبة كبيرة من الجرائم المعلوماتية ترتكب من قبل موظفي الجهة نفسها، ومن الوقائع التي حدثت في الولايات المتحدة الأمريكية أنه حكم على أحد الموظفين في إحدى شركات التأمين بالسجن لمدة سبع سنوات وغرامة مقدارها ١٥٠ ألف دولار لأنه أدخل فيروساً في أجهزة الشركة التي كان يعمل فيها مما أدى إلى ضياع ١٦٠ من سجلات العملاء، وذلك انتقاماً من الشركة لأنها قامت بفصله من العمل[٢].كما توجد هنالك العديد من الوسائل الإلكترونية التي تمنع الأشخاص للدخول غير المصرح لهم؛ كبرامج جدار النار والبطاقات الممغنطة، وبرامج مكافحة الفايروسات، وذلك على النحو التالي[٣]:

١. **الجدار الناري:** وهو عبارة عن برامج تقوم بتتبع صلاحيات وحدود المستخدم في الدخول، وإدخال المستخدم المصرح له بالدخول من خلال الرمز السري، ولها العديد من المميزات منها

(1)Behrouz A. Forouzan,"Introduction to cryptography and network security",Cryptography and network security",Publisher by New York, NY : McGraw-Hill Higher Education, 2008, P.301.

(2)AGSOUS Naima," cybercriminalite : les reseaux informatiques revue de la gendarmerie , N29 November, 2008, P.21.

(٣) قصي أيمن البداودة، المرجع السابق، ص٢٨، ٢٩.

حماية، وتأمين البيانات الموجودة على الحاسب الآلي، وتقوم في تشفير البيانات عند انتقالها بين الدوائر الرسمية، كما أنها توفر الحماية اللازمة لحماية البينات المخزنة.

٢. **البطاقات الممغنطة:** وهي تقنية أجهزه متطورة تساعد في الحد من المستخدمين، وإمكانية دخول المستخدمين للشبكة، وبذلك فإن إمكانية الدخول لا تكون إلا لحاملين هذه البطاقات.

٣. **برامج المضاده للفايروسات:** وهي البرامج التي تم تصميمها وإنشائها لأجل تدمير المعلومات الرقمية. لذلك تم تصميم برامج معدة للتصدي لهذه الأنواع من المخاطر التي تواجه الوثائق والمعلومات الخاصة بالدولة، حيث إن هذه البرامج تقوم في التصدي للفايروسات، وتقوم بمنع دخولها، واكتشافها والقضاء عليها قبل إحداث أي ضرر.

كما يمكن حماية الوثائق والأنظمة المعلوماتية الخاصة بالدولة من خلال ما يُعرف بالحماية المادية وغير المادية، فالحماية المادية تتضمن إجراءات التوصيلات والتمديدات بين الأجهزة بشكل آمن من خلال تمريرها عبر قنوات غير مكشوفة يصعب الوصول إليها، وعزلها داخل أنابيب بلاستيكية مع وضع أجهزه إنذار وتنبيه[١]. أما الحماية غير المادية فهي التي تتضمن ما يلي[٢]:

١. وضع عناوين للأجهزة المرتبطة بالشبكة المعلوماتية لكي يمكن التعرف عليها عند تشغيلها، ومن ثم حماية جميع العناوين والأجهزة التي تقوم بترجمة وتحويل العناوين من الأشخاص غير المصرح لهم بالاستخدام.

٢. متابعة جميع محاولات الدخول على النظام سواء كانت صحيحة أو فاشلة.

٣. تشفير البيانات عند إرسالها عبر الشبكة المعلوماتية لضمان عدم تحويرها أو الاطلاع عليها أو العبث فيها.

٤. توفير آليات الحماية بعد الدخول على النظام كالتزام المستخدم بالخروج من النظام أو إعطاء وقت محدد للمستخدمين، وإلغاء دخولهم بعد المدة.

٥. توفير نظام احتياطي وهو عبارة عن إجراء نسخة من الملفات الرقمية المهمة أو ملفات نظام التشغيل للحاسب الآلي بغرض حفظها من الضياع في حال فقدان الملفات الأصلية عند الحاجة لها لأي سبب كان كفقدانها مثلًا في حال تلف الحاسب أو بغرض استعادة حالة نظام التشغيل إلى وضع سابق لأي سبب كان كتعرض الحاسب للإصابة ببرمجية روتكيتسRootkits الخبيثة.

---

(١) د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، ١٩٩٢م، ص٦٢.

(٢) د. سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م، ص١١٢ وما بعدها.

المبحث الثاني

أركان جرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة

تمهيد وتقسيم:

لا تختلف الجريمة المعلوماتية عن بقية الجرائم الأخرى التقليدية، والتي يلـزم لتحققهـا تـوافر الأركان المتفق على ضرورة وجودها لتكتمل الجريمة، حيث تُعد أركان الجريمة الأساس والأصل لقيـام أي جريمة، والمشرع يتطلب لقيام الجريمة توافر أركانها المادي والمعنوي، وبدون هذين الـركنين لـا تقوم الجريمة. بينما يرى البعض الآخر أن أركان الجريمة ثلاثة أركان عامة هي: الـركن الشـرعي، والركن المادي، والركن المعنوي [1].

ولما كانت جريمة الاعتداء على الأنظمة المعلوماتية في التشريع المصري جريمة مستقلة بذاتها في نص خاص، بينما تتمثل تلك الجريمة في عدة صور في التشريعات الأخرى الأمر الذي يتعين معـه بيان أركان تلك الجريمة في التشريع المصري، ثم بيان أركان تلك الصور في التشـريعات المقارنـة، وذلك من خلال ما يلي:

المطلب الأول: الركن المادي في جريمة الاعتداء على الأنظمة المعلوماتية للدولة.

المطلب الثاني: الركن المعنوي في جريمة الاعتداء على الأنظمة المعلوماتية للدولة.

---

(١) د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠٠٩م، ص٩٨.

المطلب الأول

الركن المادي في جريمة الاعتداء على الأنظمة المعلوماتية للدولة

تمهيد وتقسيم:

تتخذ الجريمة المعلوماتية من الفضاء الافتراضي مسرحاً لها، مما يجعلها تتميز بخصوصيات تنفرد بها، إلا أن ذلك لا يعني عدم وجود تشابه لها مع الجريمة المرتكبة في العالم التقليدي أو المادي، فهي تشترك بوجود الفعل غير المشروع، ومجرم يقوم بهذا الفعل، وبالتالي لا يختلف مفهوم الركن المادي في الجريمة المعلوماتية عما تقدم. إذ ينطلق مبدأ تحديد الفعل غير المشروع وإعطائه صفة الجريمة بتحديد الركن المادي فيه، فلا جريمة دون ركن مادي، والركن المادي في الجريمة المعلوماتية يتمثل في السلوك الذي يقوم به الجاني من أجل تحقيق غاية ما، ويحدد له القانون العقاب اللازم، وهو يتباين بتباين الجرائم المرتكبة من قبل الجاني، شريطة أن يكون له مظهر خارجي ملموس، غير أن تحديد الركن المادي في الجرائم المعلوماتية تكتنفه العديد من الصعوبات خاصة فيما يتعلق بتحديد النتيجة الإجرامية والرابطة السببية؛ الأمر الذي يتعين معه تقسيم هذا المطلب إلى فرعين، وذلك من خلال ما يلي:

الفرع الأول

السلوك الإجرامي في جريمة الاعتداء على الأنظمة المعلوماتية للدولة

يُعد السلوك الإجرامي أهم عناصر الركن المادي لأي جريمة، لأنه يكشف عن سلوك مخالف لإرادة المشرع، ويبدو بمظاهر مادية ملموسة في العالم الخارجي، ويعني ذلك أن الأفكار داخل النفس لا عقاب عليها. غير إنه لما كان الجاني في الجرائم المعلوماتية يختلف عن الجاني في غيرها من الجرائم من حيث كونه ذو خبرة كافية في مجال استخدام التقنيات الحديثة، فإن السلوك الإجرامي الذي سيصدر منه في مجال ارتكاب الجريمة الإلكترونية حتماً سيختلف عن الجاني التقليدي [1].

ويثور التساؤل حول ما إذا كان العمل أو الفعل التحضيري في الجرائم المعلوماتية ومنها الجريمة محل الدراسة يُعد جريمة أم لا؟. وللإجابة على هذا التساؤل؛ فإنه يمكن القول أن العمل التحضيري وفي معظم الجرائم لا يُشكل جريمة معاقب عليها القانون إلا إذا اعتبر العمل التحضيري جريمة، أو فعلًا غير مشروع يُعاقب عليه كأن يقوم شخص بشراء سلاح ناري دون ترخيص ليقتل

---

(١) نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية، ٢٠٠٦م، ص٤٥.

شخصاً آخر. إلا أنه لم يقم بارتكاب جريمة القتل، فالعمل التحضيري في هذه الجريمة هو شراء السلاح وبدون ترخيص، وهذا مُعاقب عليه حسب قوانين حيازة الأسلحة والذخائر النارية في غالبية دول العالم.

ويُلاحظ أنه ليس كل جريمة تستلزم وجود أعمال تحضيرية، إلاّ أنه يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في الجرائم المعلوماتية –حتى ولو كان القانون لا يعاقب على الأعمال التحضيرية –ففي مجال تكنولوجيا المعلومات فإن الأمر يختلف بعض الشيء، فشراء برامج اختراق، ومعدات لفك الشفرات وكلمات المرور، وحيازة صور دعارة للأطفال فمثل هذه الأشياء تمثل جريمة في حد ذاتها.

ويرى الباحث أن الفعل غير المشروع أو النشاط المادي يُعد عنصراً مهماً من عناصر الركن المادي للجريمة المعلوماتية بشكل عام والجريمة محل الدراسة بشكل خاص، فلا جريمة دون سلوك أو فعل غير مشروع، ويتمثل النشاط المادي في الجريمة المعلوماتية– بوجه عام– في الدخول غير المشروع في نظم وقواعد معالجة البيانات والأنظمة الخاصة بالدولة، سواء ترتب عن هذا الدخول غير المشروع تلاعب بهذه البيانات أم لا، إذ أن مجرد الدخول غير المشروع لمواقع المعلومات والبرامج الحكومية يُعد جريمة مرتكبة عبر الإنترنت، وقد يتخذ هذا النشاط الإجرامي عدة صور كانتهاك السرية لخصوصية للبيانات الشخصية والإضرار بصاحبها والاطلاع على المراسلات الإلكترونية، والإدلاء بالبيانات الكاذبة في إطار المعاملات والعمليات الإلكترونية كل ذلك يُعد من صور الركن المادي للجريمة محل المعلوماتية، **وبالتالي يتحقق الركن المادي في جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة في القانون المصري من خلال صور السلوك الإجرامي التالية:**

أ. **الدخول غير المشروع:** يتحقق الركن المادي بالدخول غير المشروع، ويستوي أن يكون الدخول عمداً أو بخطأ غير عمدي. ومن ثم يتحقق الركن المادي للجريمة بمجرد الدخول بدون وجه حق ولو لم يقم الجاني بأي نشاط آخر عقب هذا الدخول كحذف البيانات أو العبث بها.

ب. **تجاوز حدود الحق المخول في الدخول:** يتحقق الركن المادي بتجاوز حدود الحق المخول في الدخول كما سبق أن أشرنا، ويستوي لدى القانون أن يكون هذا التجاوز في حدود الحق المخول له من حيث الزمان أو مستوى الدخول.

ج. **البقاء غير المشروع:** يتحقق الركن المادي بفعل البقاء بدون وجه حق على النحو السالف الإشارة إليه سابقًا.

د. **الاختراق:** يتحقق الركن المادي بفعل الاختراق، وهو ما يختلف عن الدخول بأن الأخير يكون بفتح جهاز الحاسب الآلي أو باستخدام كلمة سر أو رمز أو كود سري، بينما الاختراق يكون

بأية وسيلة أخرى، كأن يكون ذلك باستخدام برامج متخصصة لاختراق المواقع والأنظمة المعلوماتية والحسابات الشخصية.

ويقصد بعدم مشروعية الدخول هنا: انعدام سلطة الجاني في الدخول إلى النظام المعلوماتي مع علمه بذلك، وهذا يتطلب أساساً معرفة صاحب الحق في الدخول إلى هذا النظام، ويمكن القول إن الدخول إلى جهاز حاسوبي أو منظومة معلوماتية أو موقع إلكتروني يعد غير مشروع في الحالتين التاليتين:

الحالة الأولى: إذا كان دخول الفاعل إلى إحدى هذه الأنظمة المعلوماتية قد تم دون الحصول على تصريح من الشخص المسئول عن النظام. **والحالة الثانية:** إذا كان الفاعل مصرح له بالدخول إلى إحدى هذه الأنظمة ولكنه تجاوز هذا التصريح الممنوح له بالوصول إلى معلومات لا يشملها التصريح.

وغالباً ما يتم الدخول غير المصرح به في الحالة الأولى من قبل أشخاص خارج الجهات المجني عليها التي يوجد فيها النظام المعلوماتي المخترق، أما في الحالة الثانية فإن من يتجاوز التصريح الممنوح له بالوصول إلى معلومات هو غالبا شخص من داخل الجهة المجني عليها، ويصعب في هذه الحالة الأخيرة معرفة ما إذا كان العامل في هذه الجهة قد تجاوز بالفعل حدود اختصاصه[1]. **وبالتالي يتعين تحديد اختصاصات العاملين في مثل هذه الجهات تحديداً دقيقاً حتى يسهل تحديد التجاوزات في الصلاحية.**

ويُعد الدخول غير مشروعاً متى ثبت عدم رضاء صاحب الحق في استعمال نظام الكمبيوتر بتمكين الغير–الجاني–من الدخول إلى هذا النظام، ويُعتبر عنصر عدم الرضاء متوافراً إذا علق صاحب النظام استخدام ذلك النظام على دفع اشتراك مالي معين نظير الاستفادة من الدخول إلى هذا النظام، فتقع الجريمة ممن يقوم بالدخول إلى هذا النظام دون تسديد المقابل المالي الذي حدده صاحب النظام نظير هذه الخدمة[2]، وبالتالي فإن الدخول المشروع هو الذي يكون من قبل المستخدم أي المالك، أو المسؤول عن هذا النظام، أو الموقع أو الشبكة الإلكترونية، أو الشخص المصرح له من قبل المستخدم المالك أو المسؤول عن النظام أو الشبكة المعلوماتية، كما قد يتم السماح للشخص بأن يدخل للنظام أو الشبكة لكن قد يتجاوز الإذن المسموح به، وهنا تقوم الجريمة بمجرد تجاوز الدخول المصرح

---

(١) د. نائلة قورة، جرائم الحاسب الاقتصادية، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٠٤م، ص٣٣٣.

(٢) د. محمود أحمد طه، المرجع السابق، ص٢٧.

به، كأن يكون مسموح له بالدخول إلى النظام لفترة زمنية محددة، ويتجاوز المستخدم هذه الفترة الزمنية، وهنا نكون أمام جريمة يعاقب عليها القانون[٣].

ويتجه البعض من الفقه[٤] للقول بأن وجه التمييز بين كل من الدخول والاختراق أن الدخول غير المشروع كان يقصد به الدخول من جانب أحد المتعاملين مع المواقع الإلكترونية أو البريد الإلكتروني أو الحساب الخاص أو النظام المعلوماتي الذي يخص الدولة من الموظفين العموميين العاملين لديها، ومن المصرح لهم بالتعامل معها، فيخالف القواعد والتعليمات الخاصة بالدخول أو البقاء، بينما الاختراق فيكون من غير العاملين بالدولة المصرح لهم بالتعامل مع هذه المواقع الإلكترونية أو الحسابات أو النظم المعلوماتية، كأن يكون شخصاً أجنبياً يحاول الدخول إلى هذه المواقع أو الحسابات أو الأنظمة المعلوماتية الحكومية.

نخلص مما تقدم أن تحديد الركن المادي في الجرائم المعلوماتية عموماً يثير جملة من الصعوبات التي تفرضها طبيعة الوسط الذي تتم فيه الجريمة والمتمثل في الجانب التقني، وهذا ما يميز ركنها المادي، الذي يجب أن يتم باستخدام أجهزة الحاسب الآلي أو الشبكة العالمية للإنترنت، ومن هنا تبدأ التساؤلات التي تتعلق ببداية النشاط التقني أو الشروع فيه، ومكان البداية واكتمال الركن المادي، وأجزاء السلوك الإجرامي المرتكب في العالم المادي، أو العالم الافتراضي، وغيرها من التساؤلات التي تتعلق بطبيعة الجريمة، **ولا شك أن السلوك الإجرامي في الجريمة المعلوماتية محل** الدراسة **يرتبط بالمعلومة المخزنة داخل الحاسب الآلي أو انتهاك الخصوصية التي قررها المشرع لهذه المعلومات والبيانات، وقد يتحقق السلوك الإجرامي بمجرد ضغط زر في الحاسب الآلي فيتم تدمير النظام المعلوماتي أو حصول التزوير أو الإتلاف أو السرقة عن طريق التسلل إلى النظام المعلوماتي الخاص بالدولة** [٥].

وباستقراء النصوص التشريعية المقارنة يتضح أنه يتمثل النشاط الإجرامي أو السلوك في جريمة الدخول غير المشروع إلى منظومة معلوماتية بفعل (الدخول)، ويقصد بالدخول هنا: جميع الأفعال التي تسمح بالولوج إلى نظام معلوماتي والوصول إلى المعلومات المخزنة به، وفعل الدخول يمكن أن يتم بطريقة مباشرة إلى الحاسوب أو منظومة معلوماتية، أي بالدخول كمستخدم دون أن يكون للفاعل الحق أو التصريح للقيام بذلك. كما يمكن أن يتم الدخول بطريقة غير مباشرة أي عن بعد عن

---

(٣) د. عبد الله ذيب عبد الله، جريمة الدخول غير المشروع وفقًا للقرار بقانون رقم ١٠ لسنة ٢٠١٨م بشأن الجرائم الإلكترونية الفلسطيني، مجلة جامعة القدس المفتوحة للبحوث الإنسانية والاجتماعية، جامعة القدس المفتوحة، فلسطين، العدد ٤٨، مارس ٢٠١٩م، ص١٠.

(٤) د. رامي متولي القاضي، المرجع السابق، ص١٠٦٧، ١٠٦٨.

(٥) د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص١١٣، ١١٤.

طريق الشبكات كالإنترنت، وغالبًا ما يتم الدخول بالطريقة المباشرة من قبل العاملين في الجهات المجني عليها، أما الطريقة غير المباشرة فيرتكبها أشخاص لا ينتمون إلى هذه الجهات [٦].

نخلص من ذلك إلى أن جريمة الدخول غير المشروع هي جريمة خطر وليست جريمة ضرر أي تعد جريمة تامة بمجرد ارتكاب النشاط الإجرامي، وبناءً عليه فإن الجريمة تقع بمجرد التداخل عمداً في نظام الكمبيوتر بدون موافقة صاحبه، حتى وإن لم يجد في الملفات ما يبحث عنه من معلومات [٧].

أما جريمة التجسس المعلوماتي فإن محل السلوك الإجرامي فيها هو المعلومات التقنية المعالجة آليًا بأحد طرق ووسائل المعالجة المعلوماتية، أيًا كان نوعها شريطة أن تتسم بطابع السرية، وهذا الطابع الذي يحيلها من مجرد معلومات تقنية عادية متاح للكافة إلى معلومات تحرص الدولة على عدم اطلاع الغير عليها، أو إبقائها في إطار ضيق من الاطلاع [٨]. فالفاعل يسعى إلى الكشف عن الأسرار بغض النظر عن طبيعة هذه الأسرار أو معناها أو جهتها أو صاحبها أو قيمتها، المهم أن تتمتع تلك المعلومات بخاصية الإخفاء ومشتملات المعنى الواضح للسر، والذي لا يجوز الاطلاع عليه، إلا من قبل فئة محددة محصورة وضمن قواعد وأصول مرعية، غير قابلة للنشر تضمن حماية تلك السرية [٩].

وفيما يتعلق بجريمة الإتلاف والتدمير المعلوماتي؛ فإن النشاط الإجرامي فيها هو فعل الإتلاف، أي كل فعل من شأنه أن يؤثر في مادة الشيء أو قيامه بوظائفه المختلفة على نحو يذهب من قيمته على النحو غير المعتاد لقيمة الشيء مع مرور الزمن مع قصد الإضرار بالغير، ويُعد قيمة الشيء هو محل الحماية الحقيقي وليست مادته، حيث إن مادته هي الوسيلة لحماية قيمته، والإتلاف والتدمير والتخريب هي مصطلحات مرادفة، لأنها تدل على جعل الشيء غير صالح للاستعمال في الغرض المخصص له [١٠]، ويُقصد بعدم الصلاحية للاستعمال جعل الشيء لا يقوم بوظيفته المرصود لها على النحو الأكمل، والتعطيل هو توقف الشيء عن القيام بوظيفته فترة مؤقتة، ويكفي أيًا من هذه الأفعال حتى يقوم الركن المادي لتلك الجريمة، فالاختلاف بين الإتلاف والتعييب اختلافًا كمي يتعلق بمدى ما يترتب على الفعل من ضرر بالنسبة لمادة الشيء وقيمته، علمًا بأنه ليس بشرط في الركن المعنوي، فلا

---

(٦) د. نائلة قورة، المرجع السابق، ص٣٢٢.

(٧) د. محمود أحمد طه، المرجع السابق، ص٢٧.

(٨) د. نور سليمان يوسف يعقوب البالول، المرجع السابق، ص٣٥٨.

(٩) د. أسامة المناعسة ود. جلال الزعبي، جرائم الحاسب الآلي، دار وائل للنشر، الأردن، ٢٠٠١م، ص٣٠١.

(١٠) د. أحمد فتحي سرور، الوسيط في قانون العقوبات، القسم الخاص، الطبعة الرابعة، دار النهضة العربية، القاهرة، ١٩٩١م، ص٣٠٣؛ د. رمسيس بهنام، الجرائم المضرة بالمصلحة العمومية، منشأة المعارف، الإسكندرية، ١٩٨٥م، ص٢٤٤.

يُشترط في الإتلاف أن يكون تاماً، بل يمكن أن يكون جزئياً، ولكن يُشترط في حالة الإتلاف الجزئي أن يكون من شأنه جعل الشيء غير صالح للاستعمال أو تعطيله(١١).

ويُلاحظ أن المشرع المصري قد جرم فعل الإتلاف وعاقب عليه ووضح صور الركن المادي في المادة ٣٦١ العقوبات. كما جرم المشرع الفرنسي فعل الإتلاف بمقتضى المادة ٤٣٤ عقوبات. غير إن المادة آنفة الذكر تتعلق بإتلاف الأموال المادية دون الأموال المعنوية (أي اللامادية) مما دعا المشرع الفرنسي إلى توسيع دائرة الحماية لكي تشمل الأموال المعنوية كالبرامج وغيرها، وذلك في التعديل الصادر عام ١٩٨٨م، الذي جاء بالمادة ٤/٤٦٢ من القانون المُشار إليه(١٢).كما نصت المادة ٣/٤٦٢ من ذات القانون الواردة في نفس التعديل على تجريم كل من يقوم بالإتلاف المعلوماتي المادي. كما جرّم المشرع العُماني إتلاف المكونات المنطقية لأنظمة الحاسب الآلي في البند السادس من المادة ٢٧٦ مكرر.

ومن خلال النص السابق يتبن للباحث أن المشرع العماني في تجريمه لهذا السلوك الإجرامي حدد؛ ثلاث صور هي: **الإتلاف:** ويعني إفناء هذه المعلومات وإهلاكها كليا أو جزئيًا، **والمحو:** ويقصد به إزالة كلية أو جزئية للمعطيات المسجلة على دعامة أو الموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة، **والتغيير:** ويقصد به تغير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى.

ومن الملاحظ أن المشرع العُماني-كغيره من التشريعات المقارنة-لم يحدد الجهة التي يتبع لها معالجة البيانات فهو لم يضع شروطًا تتعلق بطبيعة البيانات والمعلومات محل الإتلاف، ولم يشترط تبعيتها لجهة معينة، وإنما جاء النص عامًا ليشمل كافة أنواع المعلومات والبيانات سواء أكانت تابعة لجهة حكومية أو خاصة. كما يمكن القول بأن النصوص التشريعية آنفة الذكر قد أوضحت أن للركن المادي في جريمة الإتلاف العمدي -في صورتها التقليدية-صور متعددة ذكرتها التشريعات ومنها(١٣):

١. **التخريب:** وهو أحد الأنشطة التي يتم بها الإتلاف (أحد صور الركن المادي للجريمة) والذي إذا انصب على المال جعله غير قابل للإصلاح (للاستعمال) أي أفقده صلاحيته للاستعمال.

٢. **الإتلاف:** يختلف هذا النشاط عن الذي سبقه في أنه إذا نصرف إلى المال أثر فيه وذلك بإنقاص صلاحيته للاستعمال إلا أنه (المال) يبقى قابلا للاستعمال.

---

(١١) د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، جرائم الأموال الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، ١٩٩٢م، ص١٥٤.

(١٢) د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٣م، ص٢٥٧.

(١٣) د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، المرجع السابق، ص٣٠٩، ٣١٠.

٣. **جعل الشيء غير صالح للاستعمال:** وبهذا النشاط يتم إعدام صلاحية المال المنقول للاستعمال ومن الممكن إلحاقه بالتخريب.

٤. **تعطيل الشيء:** ويتمثل بإعاقة الشيء (المال) عن العمل إما بشكل كلي أو جزئي.

ويُلاحظ أن صور النشاط الإجرامي آنفة الذكر تُعد عنصراً من عناصر الركن المادي لجريمة الإتلاف العمدي، وبالتالي تتوافر جريمة الإتلاف متى ما وقع إتلافاً أو تخريباً من شأنه أن يؤدي إلى فقدان قيمته كلياً أو جزئياً أي على كل المال أو بعضه، وهي صور محدودة والتي أخذ بها المشرع المصري، وهي من شأنها إتلاف ماديات الحاسب فقط، إلا أن هناك صور أخرى للركن المادي من شأنها إتلاف الأموال المعلوماتية المعنوية (البرامج والكيانات المنطقية)، والتي يغلب عليها الجانب الفني حيث استحدثتها التقنية الحديثة، **وتتمثل تلك الصور بالآتي:**

١. **التعديل غير المشروع للمعلومات:** الذي يعد من أكثر صور الإتلاف شيوعاً وهو كان تغيير غير مشروع للبرامج والكيانات المنطقية باستخدام إحدى وظائف الحاسب الآلي، وقد نصت قوانين بعض الدول على هذه الصورة مع اختلاف في التعبير [١٤].

٢. **تدمير المعلومات:** والذي يعد أبعد أثراً من مجرد إجراء بعض التعديلات للمعلومات، لقد جاءت كل القوانين التي نصت على تجريم الإتلاف المعلوماتي (إتلاف المعلومة) بلفظي إخفاء المعلومة ومحوها للتعبير عن تدمير المعلومات.

ويُلاحظ أن المشرع المصري عندما نص على جريمة الإتلاف المعلوماتي؛ فإنه لم يقيد النشاط الإجرامي بوسيلة معينة، مما يعني أن هذه الجريمة تدخل ضمن نطاق الجرائم ذات القالب الحر، كما أن النص اتسم بتعدد النتائج التي جرمها المشرع، وهي: إتلاف تلك البيانات أو المعلومات أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي أو البريد الإلكتروني, أو تدميرها أو تشويهها أو تغييرها أو تصميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها, أو إلغاؤها كلياً أو جزئياً, بأي وسيلة كانت[١٥]، وهو ما قرره كذلك المشرع العماني لكن بشكل محدود[١٦].

كما يُلاحظ أخيراً أن المشرع المصري لم يجرم نتيجة واحدة، بل جرم نتائج متعددة، وهي الإتلاف والتخريب، والتشويه، والتغيير، أو النسخ، أو التسجيل، أو تعديل المسار، أو إعادة النشر، أو الإلغاء الكلي أو الجزئي، ولا يُعد إتلافاً أو تعييباً استعمال الشيء دون رضاء مالكه، ولكن على الوجه

---

(١٤) د. نائلة قورة، المرجع السابق، ص٢١٨، ٢١٩.

(١٥) الفقرة الأخيرة من المادة ٢٠ من قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨م.

(١٦) المادتان ٩، ١٣ من قانون مكافحة جرائم تقنية المعلومات العماني رقم ١٢ لسنة ٢٠١١م.

المعد له، ما لم يكن استعمالًا مفرطًا من قيمته، أما استعمال الشيء في غير الوجه المعمد له فيعد عيبًا، إذا أفضى ذلك إلى الانتقاص من قيمته[١٧].

(١٧) د. محمد نصر محمد عوض القطري، المرجع السابق، ص١٥٠.

الفرع الثاني

النتيجة الإجرامية وعلاقة السببية

إن الجريمة المعلوماتية كغيرها من الجرائم التي يُفترض وجود النتيجة الإجرامية فيها كعنصر من عناصر الركن المادي للجريمة، وتختلف النتيجة الإجرامية في الجريمة المعلوماتية بحسب نوع الجريمة المرتكبة، حيث إن الجرائم المعلوماتية تتنوع وتتعدد لذلك فالنتيجة الإجرامية تختلف باختلاف نوع الجريمة المعلوماتية المقترفة.

ويُلاحظ مما تقدم أن الركن المادي في جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة يتطلب وجود بيئة رقمية واتصال بالإنترنت، ويتطلب أيضاً معرفة بداية هذا النشاط والشروع فيه، ونتيجة فمثلًا يقوم مرتكب هذه الجريمة بتجهيز الحاسب الآلي لكي يحقق له حدوث الجريمة، فيقوم بتحميل برنامج اختراق أو أن يقوم بإعداد هذا البرنامج بنفسه، كما يمكن أن يقوم بتلك الجريمة عن طريق إعداد برامج فيروسات تمهيداً لبثها، وبالتالي قد يعاقب الجاني في هذه الجريمة لمجرد التحضير للجريمة، وذلك بشراء برامج التجسس والاختراق ومعدات فك الشفرات وكلمات المرور.

وقد تتمثل النتيجة الإجرامية في الجريمة محل البحث في تحريف الحقيقة في البيانات والمعلومات الموجودة في جهاز الحاسوب أو الموقع الإلكتروني الخاص بالدولة، فالنتيجة هي الأثر المادي المترتب على القيام بالفعل أو النشاط المادي غير المشروع، وهي أيضاً الأثر القانوني الذي يمثل اعتداءً على المعلومات الخاصة بالدولة بتعديلها أو حذفها أو تحريفها بما يخالف القانون(١٨).

وفيما يتعلق بالنتيجة الإجرامية في جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة؛ فإنها تثير مشاكل عدة، فهل تقتصر على العالم الافتراضي، أم أن لها جزءاً في العالم المادي؟، وهل تقتصر النتيجة على مكان واحد أم تمتد لتشمل دولًا وأقاليم عدة، **فعلى سبيل المثال** إذ قام أحد المجرمين في أمريكا اللاتينية باختراق جهاز خادم أحد البنوك في سلطنة عُمان، وهذا الخادم موجود في الصين فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت الجهاز الخادم في الصين.

وتُعد علاقة السببية عنصراً مهماً من عناصر الركن المادي للجريمة، فهي حلقة وصل بين السلوك الإجرامي والنتيجة الإجرامية، وذلك بأن يثبت أن هذا السلوك هو سبب تلك النتيجة الإجرامية،

---

(١٨)عبر عنه المشرع المصري بالإتلاف لتلك البيانات أو المعلومات أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي أو البريد الإلكتروني, أو تدميرها أو تشويهها أو تغييرها أو تغييرها أو تصميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها, أو إلغاؤها كليًا أو جزئيًا, بأي وسيلة كانت حسبما ورد بالمادة ٢٠ من القانون رقم ١٧٥ لسنة ٢٠١٨م.

كذلك فإن علاقة السببية تساهم في تحديد نطاق المسؤولية الجنائية، واستبعاد المسؤولية إذا لم ترتبط النتيجة الإجرامية بالفعل[١٩]، وقد نستطيع تطبيق القواعد المطبقة على الجرائم العادية على الجرائم المعلوماتية، فيما يتعلق بعلاقة السببية إذا انطبقت عليها، ففي الجريمة محل الدراسة نجد أن فعل الدخول غير المشروع أو تجاوز حدود الحق المخول في الدخول أو البقاء غير المشروع أو الاختراق يتحقق بالنشاط المادي الصادر عن الجاني وهو ليس في حاجة لاستعمال العنف لتحقق النتيجة إذ تتحقق النتيجة لمجرد إتيانه أحد صور هذا السلوك، وبالتالي فإن رابطة السببية متوافرة بين نشاطه المادي والنتيجة الإجرامية.

ولا شك أن تحديد رابطة السببية في مجال أضرار الجرائم المعلوماتية يُعد من المسائل الصعبة والمعقدة بالنظر إلى تعقيدات صناعة الحاسوب وشبة الإنترنت، وتطور إمكانياتها، وتسارع هذا التطور، إضافة إلى تعدد وتنوع أساليب الاتصال بين الأجهزة الإلكترونية، وتعدد المراحل التي تمر بها الأوامر المدخلة حتى تخرج وتنفذ النتيجة المراد الحصول عليها، كل ذلك سيؤدي حتماً إلى صعوبة تحديد السبب أو الأسباب الحقيقية للإساءات المرتكبة في هذه المسؤولية[٢٠].

أما النتيجة الإجرامية في جريمة الدخول غير المشروع إلى منظومة معلوماتية فإنها قد تبدو وكأنها مندمجة في النشاط الإجرامي المتمثل بفعل (الدخول)، فلم يشترط أن ينجح الفاعل في الوصول إلى المعلومات المخزنة لتحقق هذه الجريمة، وإنما يكفي أن يلج إلى النظام المعلوماتي، لأن علة التجريم تتمثل في حماية النظام ذاته من الدخول إليه دون وجه حق.

ورغم أن جريمة الدخول غير المشروع إلى النظام المعلوماتي من جرائم النشاط، فإنه يمكن تصور الشروع في ارتكابها، عندما لا يتمكن الفاعل من الدخول إلى النظام المعلوماتي لظروف خارجة عن إرادته، وقد يرجع ذلك إلى أن المتهم قد تم ضبطه بعد تشغيل الجهاز وقبل أن يتمكن من فتح أي ملفات من الملفات المدونة بالنظام المعلوماتي، وقد يرجع عدم تمكن المتهم من الدخول إلى الملفات رغم فتح جهاز الحاسب الآلي معلقاً على استعمال كلمة السر، ولم يكن المتهم يعرفها [٢١].

ولا يكفي لقيام الركن المادي في جريمة الدخول غير المشروع للنظام المعلوماتي الخاص بالدولة توافر السلوك الإجرامي والنتيجة المعاقب عليها، بل يلزم إضافة لذلك أن تكون هناك علاقة سببية بينهما، وهي تلك الرابطة التي دفعت إلى الإتيان بهذا الفعل، وما يترتب عليه من نتيجة، ولكي

---

(١٩) د. لورنس سعيد أحمد الحوامدة، الجرائم المعلوماتية: أركانها وآلية مكافحتها: دراسة تحليلية مقارنة، مجلة الميزان للدراسات الإسلامية والقانونية، جامعة العلوم الإسلامية العالمية، عمان، الأردن، المجلد ٤، العدد١، يناير ٢٠١٧م، ص٢٠٦.

(٢٠) منصور بن صالح السلمي، المسؤولية المدنية لانتهاك الخصوصية في نظام مكافحة جرائم المعلوماتية السعودية، رسالة ماجستير، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، ٢٠١٠م، ص٧٥، ٧٦.

(٢١) د. محمود أحمد طه، المرجع السابق، ص٣٢.

يكون الجاني مسئولًا قانونيًا لارتكاب الفعل يجب أن تكون هناك نتيجة حتمية لذلك الفعل، وفي حال انتفاء هذه العلاقة لا تكون هناك علاقة سببية، وبالتالي؛ لا يكون مسئولًا جنائيًا وقانونيًا عن نتيجة الفعل(٢٢).

ولا شك أن رابطة السببية في الجرائم المعلوماتية أساسية لتحديد نطاق المسؤولية الجنائية في كافة صور جرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة العمدية، وتقوم العلاقة السببية في تلك الجرائم على البحث في الصلة بين مرتكب الجريمة والفعل الذي ارتكبه وبين الآلة. فالعلاقة التقنية بين مرتكب الجريمة وبين الآلة محل الجريمة المعلوماتية هي الأساس لبيان رابطة السببية في الجرائم المعلوماتية، ويقع عبء إثبات وجود تلك الرابطة من عدمها على النيابة العامة، بما يقدم إليها من أدلة وبينات واستماع للشهود في مثل هذا النوع من الجرائم المستحدثة، والتي تحتاج إلى أدلة إثبات أخرى تختلف وأدلة الإثبات التقليدية.

ويرى الباحث أن المشرع المصري كان موفقًا عن نظيره العُماني، فيما يتعلق ببيان الركن المادي لجريمة الإتلاف المعلوماتي، حيث وسع المشرع المصري من صور الركن المادي في هذه الجريمة، وذلك بإدخال صور متعددة للركن المادي تكون صالحة أساسًا لإتلاف المعلومات، مثل: الإتلاف–التدمير، التشويه، التغيير، التصميم، النسخ، التسجيل، تعديل المسار، إعادة النشر، الإلغاء الكلي أو الجزئي، أو أي وسيلة كانت، بينما نجد المشرع العُماني قد حصرها في: الإتلاف، التدمير، الإيقاف أو التعطيل عن العمل. كما يحمد للمشرع المصري كذلك أنه لم يهتم بالوسيلة التي تم استعمالها في الإتلاف، حيث إن النصوص التشريعية في القانون المصري تنص على معاقبة كل من يخرب أو يتلف الأموال المعنوية أو يجعلها غير صالحة للاستعمال بأي وسيلة كانت، الأمر الذي دفع البعض من الفقه(٢٣) للقول بأنه قد ترتكب تلك الجريمة بعدة وسائل أخرى منها ما يمكن تسميتها بالوسائل التقليدية، كإطلاق العيارات النارية على الحاسب الآلي أو تفجير المركز المعلوماتي الخاص بالدولة، أو تدمير الحاسب الآلي بإدخال قطع معدنية في فتحته، أو إحراقه بالكامل، إذ تُعد تلك الصور ضربًا من ضروب الإتلاف(٢٤).

والخلاصة أن الإتلاف المعلوماتي قد يُرتكب بوسائل تقليدي من شأنها تؤدي إلى إتلاف ماديات الحاسب الآلي، وتؤثر كذلك على المعلومات التي يحويها هذا الجهاز، لكن يُلاحظ أن أثر تلك الوسائل

---

(٢٢) د. أحمد شوقي أبو خطوة، مرجع سابق، ص١٨٦.

(٢٣) د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر، المرجع السابق، ص٥٣٠.

(٢٤) د. المستشار. معوض عبد التواب، الوسيط في شرح جرائم التخريب والإتلاف والحريق، دار المطبوعات الجامعية، الإسكندرية، ١٩٨٩م، ص١٠٧.

يكون محدود، وقد يُرتكب الإتلاف المعلوماتي بوسائل فنية حديثة، لكنها قد تحقق إتلافاً معلوماتياً واسع النطاق، كاستخدام الفيروسات، وبرامج الدودة، والقنابل المنطقية أو الزمنية.

المطلب الثاني

الركن المعنوي في جريمة الاعتداء على الأنظمة المعلوماتية للدولة

تمهيد وتقسيم:

يُعد الركن المعنوي ركن أساسي في تكوين الجريمة. حيث لا تقوم الجريمة دونه، ويُعتبر الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، ويُقصد به مدى اتجاه إرادة الجاني إلى ارتكاب الجريمة. فإذا اتجهت إرادته إلى ارتكابها توافر لديه القصد الجنائي وكانت الجريمة عمدية، وإذا لم تتجه تلك الإرادة إلى ارتكابها وتوافر لديه الخطأ غير العمدي كانت الجريمة غير عمدية[٢٥].غير إنه يثور التساؤل حول ما إذا كانت المقومات التي تحكم الركن المعنوي في الجرائم التقليدية هي نفسها التي تنطبق في حالة الجرائم المعلوماتية، ومنها جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة، وبالتالي يلزم الأمر بيان الركن المعنوي في هذه الجريمة، وذلك من خلال الفرعيين التاليين:

الفرع الأول

عناصر القصد الجنائي في جريمة الاعتداء على الأنظمة المعلوماتية للدولة

يُعبر الركن المعنوي بصفة عامة عن وجود إرادة وروابط مع ماديات الجريمة دفعتها للوجود، فلا يكفي لإيقاع العقوبة على الجاني أن يقوم بارتكاب العنصر المادي فيها، وإنما يلزم إلى جانب ذلك وجود علاقة نفسية أو معنوية تربط الجاني بالنشاط الذي تم ارتكابه، بحيث يتوافر لدى الفاعل إرادة الفعل الإجرامي وإرادة النتيجة، وكل ما يتصل بالفعل من وقائع تسهم في تحديد صفته الإجرامية [٢٦].

وتأخذ هذه العلاقة صورة القصد الجنائي في الجرائم العمدية، وصورة الخطأ في الجرائم غير العمدية. فالقصد الجنائي هو توجه إرادة الفاعل نحو اقتراف الفعل الإجرامي، وإرادة تحقيق نتيجته مع العلم بصفته المحظورة[٢٧]. حيث ترتكز المسؤولية للفاعل على إتيان سلوك يُعتبر سبباً في تحقق النتيجة المحظورة قانوناً، مع ضرورة توافر رابطة نفسية بين النشاط الإجرامي الذي هو الفعل ونتائجه، وبين الفاعل الذي صدر عنه هذا النشاط، وهذه الرابطة النفسية اصطلح على تسميتها بالركن

---

(٢٥) د. غنام محمد غنام، د. تامر محمد صالح، شرح قانون العقوبات: القسم العام، بدون دار نشر، ٢٠٢٢م/٢٠٢٣م، ص٩٧.

(٢٦) د. محمود نجيب حسني، النظرية العامة للقصد الجنائي، دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العملية، الطبعة الثالثة، دار النهضة العربية، القاهرة، ١٩٨٨، ص١٢.

(٢٧) د.عوض محمد، قانون العقوبات، القسم العام، دار المطبوعات الجامعية، الإسكندرية، د. ت، ص١٤٩.

المعنوي[٢٨]، ويكتسي تحديد الركن المعنوي بالغ الأهمية في الجريمة المعلوماتية بوجه عام، كما هو الحال بالنسبة للجريمة المرتكبة في العالم المادي، حيث بموجبه يمكن تحديد مناط مساءلة الجاني، وذلك بتحديد القصد الجنائي لديه، الذي بدونه لا يمكن أن يعاقب الشخص المرتكب للفعل.

ولا يتحقق القصد الجنائي في جريمة الاعتداء على الأنظمة المعلوماتية إلا إذا كان الجاني يعلم بالعناصر الأساسية لقيام هذه الجريمة سواء تعلق ذلك بسلوكه الإجرامي أم بموضوع الاعتداء، فإذا كان الجاني جاهلًا بشيء من ذلك، فلا يتحقق القصد الجنائي، ففي الجريمة محل الدراسة فإنه لا يتحقق القصد الجنائي إلا إذا كان الجاني يعلم أنه دخل عمدًا, أو دخل بخطأ غير عمدي وبقي بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعًا أو بريدًا إلكترونيًا أو حسابًا خاصًا أو نظامًا معلوماتيًا يُدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكًا لها, أو يخصها. فالذي يدخل أحد هذه المواقع أو الأنظمة وهو يجهل ذلك، فإنه لا يتوفر القصد الجنائي قبله، وليس كل جهل ينتفي معه القصد الجنائي، بل هناك وقائع يؤثر الجهل بها في القصد، وأخرى لا يتأثر بها القصد.

ويقوم الركن المعنوي في جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة على أساس مجسد في توافر الإرادة الأثمة لدى الفاعل، وتوجيه هذه الإرادة إلى القيام بعمل غير مشروع جرمه القانون، كدخوله عمدًا, أو بخطأ غير عمدي وبقاءه بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول، أو اخترق موقعًا أو بريدًا إلكترونيًا أو حسابًا خاصًا أو نظامًا معلوماتيًا يُدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكًا لها, أو يخصها. كما يجب أن تتوفر النتيجة الإجرامية المترتبة على الأفعال السابقة، فتكتسب إرادة الجاني الصفة الجرمية.

ويُلاحظ أن جريمة الدخول غير المصرح به من الجرائم العمدية، حيث يتخذ الركن المعنوي فيها صورة القصد الجنائي العام بعنصريه العلم والإرادة[٢٩]، وهو ما أكدته العديد من التشريعات على ذلك وبصيغ مختلفة، فالمادة ١/٣٢٣ من قانون العقوبات الفرنسي تطلبت أن يتم الدخول بطريق الغش والخداع، وفي التشريع العماني يلزم أن يتم الدخول عمدًا[٣٠]. فيتعين توافر عناصر القصد الجنائي العام؛ العلم والإرادة، فيتعين إذن توافر علم الجاني بأن فعله ينصب على نظام معلوماتي بما يتضمنه

---

(٢٨) د.فتوح عبد الله الشاذلي، قانون العقوبات– القسم العام، الكتاب الأول: أوليات القانون الجنائي– النظرية العامة للجريمة، دار المطبوعات الجامعية، الإسكندرية، ١٩٩٨م، ص٤٣٣.

(٢٩) د. أشرف توفيق شمس الدين، شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة والعقوبة، طبعة خاصة لطلاب التعليم المفتوح بكلية لحقوق بجامعة بنها، دون دار نشر، ٢٠٠٩م، ص١٥٥.

(٣٠) المادة ٣ من قانون مكافحة جرائم تقنية المعلومات العماني رقم ١٢ لسنة ٢٠١١؛ المادة ١/٣٢٣ عقوبات فرنسي.

من معلومات وبرامج خاصة بالدولة، باعتباره المحل الذي يحميه المشرع، ولا يؤثر على توافر القصد الجنائي أن يقصد الفاعل الدخول إلى نظام، ثم يترتب على فعله الدخول على نظام آخر؛ لأن ذلك من باب الحيدة عن الهدف التي لا تؤثر على توافر القصد الجنائي، حيث يجهل الفاعل طبيعة فعله المتمثل بالدخول لنظام معلوماتي؛ لأن المجرم المعلوماتي في أغلب الأحوال يتوافر لديه خبرة تكنولوجية في هذا المجال، إلا أنه حال حدوث ذلك ينتفي القصد الجنائي(٣١).

كما يتخذ الركن المعنوي في جريمة التجسس المعلوماتي صورة القصد، إذ يتعين توافر عناصر القصد الجنائي العام أي العلم والإرادة، وبالتالي يتعين علم الجاني بأن فعله ينصب على نظام معلوماتي أو شبكة معلوماتية خاصة بالدولة وأجهزتها، كما يتعين أن يكون الجاني على علم بأنه يدخل موقع إلكتروني أو نظام معلومات، أو شبكة إلكترونية خاصة بالدولة، وغير مصرح له بالدخول. كما يتعين توافر عنصر الإرادة حتى يقوم القصد الجنائي، وإرادة الفعل وإرادة النتيجة المتمثلة في الدخول والتجسس غير المصرح به(٣٢).

كما تُعد جريمة الإتلاف والتدمير المعلوماتي من الجرائم العمدية، ويتخذ ركنها المعنوي صورة القصد الجنائي بعنصري العلم والإرادة، فيلزم أن يعلم الجاني أن المال الذي يقع عليه فعله مملوك للدولة، وأن من شأن فعله التأثير في مادة الشيء، أو في قيمته، أو في كفاءته، إذا ما قام بتحقيق المطلوب منه(٣٣).

وبتوافر عنصر الإرادة باتجاه إرادة الجاني إلى الفعل الإجرامي بتخريب أو إتلاف أو تدمير أو إعدام الصلاحية، أو التعطيل للمال المملوك للدولة- أو الغير أيضاً- فإذا وقع الفعل بطريقة خاطئة، فإنه يخضع لنص المادة ٦/٣٧٨ عقوبات مصري، التي تقرر عقوبة الغرامة التي لا تجاوز خمسين جنيهاً لكل من تسبب بإهماله في إتلاف شيء من منقولات الغير(٣٤)، وهو ما قرره المشرع العُماني حيث يعاقب بالسجن مدة لا تقل عن (١٠) عشرة أيام، ولا تزيد على شهر، وبغرامة لا تقل عن (١٠٠) مائة ريال عماني، ولا تزيد على (٣٠٠) ثلاثمائة ريال عماني، أو بإحدى هاتين العقوبتين كل من تسبب بإهماله في إتلاف منقول مملوك للغير(٣٥)، ولم يشترط المشرعين توافر قصد خاص في تلك الجريمة، ويكتفى في قيامها بتوافر القصد العام.

---

(٣١) د. عبد الإله محمد النوايسة، جريمة الدخول غير المشروع في تشريعات الجرائم الإلكترونية العربية: دراسة مقارنة، المجلة القانونية والقضائية، السنة (١٠)، العدد (١)، ٢٠١٦م، ص٤٧.

(٣٢) د. عبد الإله محمد النوايسة وآخرين، المرجع السابق، ص٤٧٦.

(٣٣) د. محمد نصر محمد عوض القطري، المرجع السابق، ص١٥١.

(٣٤) د. هشام محمد فريد رستم، المرجع السابق، ص٣٢١، ٣٢٢.

(٣٥) المادة ٣٧٣/ هـ من قانون الجزاء العُماني رقم ٧ لسنة ٢٠١٨م.

الفرع الثاني

صور القصد الجنائي في جريمة الاعتداء على الأنظمة المعلوماتية للدولة

للركن المعنوي صورتان، الصورة الأولى: تتمثل في القصد الجنائي أو العمد، أما الصورة الثانية: فهي تتمثل في الخطأ، وتشترك الصورتان معاً في إرادة السلوك أي أن الجاني يريد السلوك والنتيجة في القصد الجنائي، بينما تختلف الصورتان في إرادة النتيجة حيث يريد الجاني السلوك في الخطأ دون النتيجة(١).

وللقصد الجنائي صورتان:

الصورة الأولى: القصد الجنائي العام، إذ يهدف الجاني عند ارتكابه الواقعة الإجرامية مع العلم بعناصرها إلى تحقيق غرض معين، بتحقيقه قد تتم الجريمة ويتوافر لها القصد الجنائي العام، ففي جريمة القتل يكون غرض الجاني إزهاق روح المجني عليه، وفي جريمة السرقة يكون غرض الجاني حيازة المال المسروق، وفي جريمة الرشوة يكون غرض الجاني الحصول على منفعة من الراشي، وبالتالي فإن القصد الجنائي العام أمر ضروري ومطلوب في كل الجرائم العمدية.

الصورة الثانية: القصد الجنائي الخاص: إذ يلتقي القصد الخاص مع القصد العام في جميع عناصره، ويزيد عنه في تحديد الإرادة الإجرامية لدى الجاني إما بباعث معين قد يدفعه إلى الجريمة، وإما بنتيجة محددة يريدها، وحكمة هذا التحديد هي الرغبة في توضيح هذه الجريمة وتمييزها عن غيرها من الجرائم التي تشترك معها في بعض العناصر(٢)، ويتكون القصد الجنائي الخاص من عنصري العلم والإرادة بالإضافة إلى عنصر ثالث، وهو عنصر الباعث أو الغرض على ارتكاب الجريمة. فالباعث هو العامل النفسي أو القوة الدافعة التي تحرك إرادة الجاني نحو ارتكاب الجريمة(٣).
الجريمة(٣).

وبالتطبيق على جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة، نجد أن هذه الجريمة يمكن أن تقع عمداً أو بطريق غير عمدي، وهو ما أشار إليه المشرع بعبارة:" دخل عمداً أو بخطأ غير عمدي وبقي بدون وجه حق". ومن ثم فإن هذه الجريمة قد تتحقق بطريق العمد بتوافر القصد الجنائي العام بعنصريه العلم والإرادة، بأن يعلم الجاني بدخوله بدون وجه حق لموقع إلكتروني أو حساب شخصي أو نظام معلوماتي وبقاءه عليه أو تجاوزه حدود الحق المخول له في الدخول، أو باستخدامه

---

(١) د.عمر الشريف، درجات القصد الجنائي، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٠٢م، ص(أ).

(٢) د.منصور رحماني، الوجيز في القانون الجنائي العام، فقه، قضايا، دار العلوم للنشر والتوزيع، الجزائر، ٢٠٠٦م، ص١١٢.

(٣) د. محمد محرم محمد ود. خالد محمد المهيري، قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة فقهاً وقضاءً، الطبعة الطبعة الثانية، الفتح للطباعة والنشر، الإسكندرية، ١٩٩٢م، ص١٠٧.

أية برامج لاختراق ودخول هذه المواقع والحسابات، وأن تتجه إرادته إلى تحقيق ذلك، بينما في حالة الخطأ غير العمدي، فإرادة الجاني لا تتجه إلى الدخول غير المشروع للمواقع أو الحسابات أو النظم المعلوماتية، ولكن الدخول يتحقق بفعل الجاني نتيجة عدم مراعاته لقواعد أمن الحاسبات والمعلومات(١).

ويُعد قصداً جنائياً خاصاً في القانون العُماني الدخول بقصد الحصول على بيانات أو المعلومات(٢) الحكومية الإلكترونية السرية بطبيعتها أو بموجب تعليمات صادرة بذلك، وكذلك الدخول عمداً إلى موقع إلكتروني بقصد تغيير تصميمه أو تعديله أو إلغائه أو إتلافه أو شغل عنوانه(٣).

ويُعد استخدام المتهم وسائل خداعية في تحقيق الدخول أو البقاء في النظام قرينة على توافر القصد الجنائي في حقه، ويتحقق ذلك إذا كان الدخول على النظام يتطلب شفرة أو بطاقة معينة، فقام الجاني بسرقة هذه البطاقة أو بكسر هذه الشفرة، وإذا توافر القصد الجنائي فإنه لا عبرة بالبواعث التي تكون وراء قيام الجاني بفعله(٤).

ولا بد أن يعلم الفاعل أن دخوله غير مشروع أي ليس له الحق في الدخول إلى هذا النظام المعلوماتي، ولا يشترط أن ينصرف قصد الفاعل إلى النتائج المحتملة لدخوله من إتلاف للمعلومات أو إلحاق الضرر بالنظام المعلوماتي للدولة، فقد قضت الدائرة الثانية **(Second Circuit)** في محكمة نيويولك في قضية **Robert Morrise** بأن نية الدخول تكفي أن تنصرف إلى الدخول غير المصرح به، ولا يشترط أن تمتد إلى فعل إلحاق الضرر بالحاسوب(٥).

وبالتالي يُنتفى القصد الجنائي في حق المتهم إذا كان الدخول أو البقاء قد تم بطريق الخطأ، وتطبيقاً ذلك ينتفى القصد الجنائي، إذا كان الدخول إلى النظام أو البقاء فيه أو استعماله كان مشروعاً، وكذلك إذا ثبت أن الجاني قد دخل على قواعد البيانات مصادفة، وإنه كان وليد خطأ، ولم يكن فعله كاشفاً عن توافر هذا القصد، وأيضاً إذا كان الدخول على النظام يتم بموجب اشتراك، وكان قد سبق للشخص الدخول بوجه مشروع غير أنه قد انتهت مدة اشتراكه، وكان يجهل ذلك(٦).

وفي ذلك قضت محكمة جنح مستأنف **Aix- en- Provence** بإدانة أحد مندوبي شركة فرنسا للاتصالات والذي كان مكلفاً بالرقابة والإشراف على سنترال تليفوني بتهمة الدخول بطريق غير

---

(١) د. رامي متولي القاضي، المرجع السابق، ص١٠٦٨.

(٢) د. شوقي سالم، نظم المعلومات والحاسب الآلي، مركز الإسكندرية للوثائق الثقافية والمكتبات، ٢٠٠١م، ص٢٩.

(٣) المواد ٦، ٧ من قانون مكافحة جرائم تقنية المعلومات العماني رقم ١٢ لسنة ٢٠١١.

(٤) د. محمود أحمد طه، المرجع السابق، ص٣٣.

(5) Rizger M. Kadir: The Offense of unauthorized Access in Computer Crimes Legislation A Co,parative Study, Journal of ShiR & Law, Issue No. 40- October. 2009, P. 57.

(٦) د. محمود أحمد طه، المرجع السابق، ص٣٣.

مشروع إلى النظام المعالجة الآلية للمعلومات، لأنه قام بتوصيل الجهاز الميناتل بخط التجارب، وظل متصلًا بشكل مستمر بأحد مقدمي الألعاب التليميانية الذي كان يمنح جوائز على شكل بونات شراء تتناسب مع مدة التوصيل أي أن الجوائز تزداد تبعًا لزمن الاستعمال.

وكانت تتم إزالة هذا الاستخدام غير القانوني بطريقة فنية خاصة، وكان المتهم قد أحيل إلى المحكمة بتهمة السرقة، إلا أن المحكمة لم تأخذ بهذا الكيف استنادًا إلى حكم للنقض اعتبرت فيه الاتصالات التليفونية نوع من الخدمات لا يمكن حيازتها، وانتهت المحكمة إلى إدانة المتهم عن جريمة الدخول بطريق غير مشروع إلى نظام المعالجة الآلية للمعلومات(١)، وفي حكم آخر لجنح باريس قضت بإدانة متهم عن جريمة الدخول بطريق غير مشروع إلى نظام المعالجة الآلية للمعلومات في واقعة كان المتهم يقدم نفسه على أنه مندوب المجموعة الفيدرالية لكي يحصل من الشركات على توريد خدمات تليفونية نظير مبلغ ٢٥٠ ألف دولار (٢).

نخلص مما سبق أنه يتلاقى القصد الجنائي بصورتيه العام والخاص في الجرائم المعلوماتية، ومنها الجريمة محل الدراسة مع مثيله في الجرائم التقليدية في عدة نقاط، منها العلم والإرادة، فالمجرم يجب أن يكون عالم بأن الفعل الذي يقوم به يُعتبر فعل غير مشروع، وذلك بإرادة صريحة من أجل إحداث الضرر للمجني عليه. أما القصد الخاص فيلتقي مع القصد العام في الكثير من عناصره، ويزيد عنه في تحديد الإرادة الإجرامية لدى الجاني إما بباعث معين قد يدفعه إلى الجريمة، وإما بنتيجة محددة يريدها، وحكمة هذا التحديد هي الرغبة في توضيح هذه الجريمة وتمييزها عن غيرها من الجرائم التي تشترك معها في بعض العناصر(٣).

ولبيان الفرق بين القصد الجنائي العام والقصد الجنائي الخاص في هذا الأمر؛ فإن القصد الجنائي العام يقوم على العلم والإرادة، كما يقوم القصد الجنائي الخاص على العلم والإرادة، غير أنه يمتاز عنه بأن العلم والإرادة فيه لا يقتصران على أركان الجريمة وعناصرها، وإنما يمتدان بالإضافة إلى ذلك إلى وقائع ليست في ذاتها من أركان الجريمة، وإذا تطلب القانون في جريمة توافر القصد الخاص فمعنى ذلك أنه يتطلب أولًا انصراف العلم والإرادة إلى أركان الجريمة، وبذلك يتوافر القصد العام، ثم يتطلب بعد ذلك انصراف العلم والإرادة إلى وقائع لا تُعد طبقًا للقانون من أركان الجريمة، وبهذا الاتجاه الخاص للعلم والإرادة يقوم القصد الخاص، ولقيام الركن المعنوي في الجرائم المعلوماتية

---

(1) Ca. aix-en- rovence,13 ech.,23 Oct.,1996, J.C.P., ed.,E.,28 mai.1998.

مشار إليه في: د. محمود أحمد طه، المرجع السابق، ص٣٣، ٣٤.

(2) Trip. Corr., Paris, 13 ech., 25/2/1997, J.C.P., ed, E.,28/5/1998.

مشار إليه في: د. محمود أحمد طه، المرجع السابق، ص٣٤.

(٣) د. منصور رحماني، المرجع نفسه، ص١١٢.

ومنها الجريمة محل الدراسة فإنه، لابد أن يعلم الجاني أنه يرتكب هذه الجريمة من خلال شبكة الإنترنت كأحد الأفعال التي يتضمنها نص التجريم، وأن تتجه إرادته إلى القيام بذلك الفعل(١).

وما تجب الإشارة إليه أنه رغم التوافق بين جميع الجرائم سواء التقليدية أم المعلوماتية في وجوب توافر الركن المعنوي فيها، إلا أن هناك استثناءات فيما يخص الجريمة المعلوماتية ومنها الجريمة محل الدراسة، وذلك في ظل الطبيعة اللامادية لهذه الجريمة، والسرعة في ارتكابها، حيث لا تدع المجال لتحديد الفعل من عدمه فما بالك بتحديد القصد الجنائي فيها، بالإضافة إلى اختلاف طبيعة المجرمين، حيث ينفرد المجرمون الذين يقومون بأفعالهم غير المشروعة عبر الإنترنت عن نظرائهم في الجريمة التقليدية فيما يخص الباعث.

ويتجه البعض للقول بأنه إذا كان الركن المعنوي يختلف في الجرائم المعلوماتية باختلاف الباعث الذي يدفع الجاني لارتكاب أفعاله التي سبق وأن تم ذكرها، فليس كل المجرمين عبر الإنترنت لهم نية في الإجرام، فرغم أن هناك من المجرمين من يسعى لتحقيق أغراض مادية أو سياسية أو إيديولوجية، إلا أنه هناك من الأفراد من يقوم بأفعاله من أجل التعلم أو لمجرد التسلية في بعض الأحيان، مما يجعل في هذه الحالة تحقق شرط القصد الجنائي منعدم، ومنه لا يتوافر الركن المعنوي في هذه الجرائم(٢).

ولا يتفق الباحث مع الفكرة آنفة الذكر أو بشكل أدق لا يمكن التسليم بها في كافة الجرائم المعلوماتية، لا سيما الجرائم الواقعة على الأنظمة المعلوماتية الخاصة بالدولة، فإذا كان الباعث في الجرائم المعلوماتية من الصعوبات التي تعوق الوصول إلى تحديد العقوبة لمقترف الفعل المجرم، وذلك لانعدام القصد الجنائي، فمثلًا إذا اخترق أحد القراصنة الهواة قاعدة بيانات لشركة معينة من أجل التعلم أو من أجل التسلية دون علمه أن هذا الفعل مجرم؛ فإنه ينتفي هنا الركن المعنوي للجريمة.

غير أن الملاحظ على هذه الأفعال، وبالرغم من عدم توافر القصد الجنائي فيها، إلا أنها تسبب أضراراً وخسائر فادحة لدى الجهة المجني عليها تفوق أضرار الجريمة التقليدية، لاسيما وإن كانت هذه الجهة حكومية كما هو الشأن في الجريمة محل الدراسة، فالتسليم بالرأي آنف الذكر أي انتفاء القصد الجنائي وبالتالي يُعفي الجاني من المساءلة، ومن ثم يتم ضياع حقوق الجهة المجني عليها، ومن أجل ذلك قرر المشرع مساءلة الجاني على أساس الضرر الذي ألحقه بالجهة المجني عليها.

وبالتالي يُسأل الجاني على مجرد الدخول سواء كان عمداً أم بخطأ غير عمدي، أو بقي دون وجه حق، وتشدد عقوبته إذا ما ترتب على ذلك إتلاف تلك البيانات أو المعلومات أو ذلك الموقع أو

---

(١) منصور بن صالح السلمي، المرجع السابق، ص٧٨.

(٢) منصور بن صالح السلمي، المرجع السابق، ص٦٨.

الحساب الخاص أو النظام المعلوماتي أو البريد الإلكتروني, أو تدميرها أو تشويهها أو تغييرها أو تغييرها أو تصميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها, أو إلغاؤها كلياً أو جزئياً, بأي وسيلة كانت، وإلا ترتب على ذلك وقوع الجريمة ومن ثم يستحق الجاني العقاب المقرر للجريمة.

نخلص مما سبق أن معظم الجرائم الواقعة على أمن الدولة المعلوماتي تنطوي طبيعتها على تهديد مصلحة الدولة بإحتمال تحقق ضرر معين، لأن الاعتداء المحتمل على الحق هو في الواقع اعتداء فعلي على مصلحة جديرة بالحماية، وأن تحقيق النتيجة المادية المتجه إليها السلوك الإجرامي لا يدخل كعنصر لازم في التكوين القانوني لمعظم تلك الجرائم؛ لأنها من جرائم الخطر.

ويرى الباحث أن القصد العام والخاص في جرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة أساسي لتحديد المسؤولية الجنائية، والذي يحدد وجود قصد خاص في تلك الجرائم هو طبيعة الجريمة ونية الإضرار أو النية الخاصة للجاني والتي يمكن استشفافها من مكونات كل جريمة على حدة، وبشكل مستقل، وبالتالي فإن جرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة كغيرها من الجرائم المعلوماتية المستحدثة وكذلك الجرائم التقليدية التي يُشترط وجود الركن المعنوي لقيامها، ولا يتصور قيام أي نوع من تلك الجرائم دون وجود الركن المعنوي. أما عن الإثبات في توافر الركن المعنوي في الجرائم محل البحث فهو يقع على عاتق النيابة العامة، والمحكمة المختصة بالنظر في مثل هذا النوع من الجرائم، والمحكمة صاحبة الصلاحية بتقدير وجود سوء النية من عدمها، ووزن البينات، وتمحيصها بما لها من صلاحية باعتبارها صاحبة القرار النهائي بالفصل في الدعاوى المرفوعة أمامها.

وعليه؛ فلا يتريث المشرع لإنزال العقاب إلى أن تتحقق النتيجة الإجرامية. بل يبادر ويعجله ليرجع التجريم إلى لحظة مبكرة تُعتبر فيها الجريمة قد تمت عندها، ولو لم تكن كذلك في الحقيقة، فالمشرع وبالنظر لخطورة الجرائم مبكرة الاتمام في محيط الجرائم الماسة بأمن الدولة المعلوماتي رأى ضرورة شمول السلوك المكون لها بالعقاب على الرغم من أنه لم يصل بعد إلى حد الفعل الذي يضر بصورة مباشرة بالمصلحة المحمية في نطاق تلك الجرائم كما في حالة الاتفاق على ارتكاب جريمة ماسة بأمن الدولة المعلوماتي لأن هذه الصورة لا تدخل في نطاق التجريم والعقاب طبقًا للقواعد العامة.

ولما كانت جرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة والمساس بأمنها المعلوماتي، والاعتداء عليه يشُكل تحدياً كبيراً يواجه المشرع الجنائي في كافة المجتمعات، نظراً لضخامة الأضرار التي قد تنجم عن مثل تلك الجرائم، والتي قد تصل إلى حد انهيار مجتمع بأكمله؛ الأمر الذي أدى إلى الحاجة الملحة لمواجهة هذه الجرائم بقواعد خاصة تتميز بالشدة والردع. لذلك خص المشرع العقابي هذه الجرائم بسياسة جنائية تختلف عن الجرائم الأخرى، ويأتي ذلك من منطلق خطورة هذه الجرائم، وأهمية المصلحة التي يستهدف المشرع حمايتها؛ لذلك اعتمد المشرع على السياسة التحوطية، وقد ظهر ذلك بوضوح في بعض الجوانب المتعلقة بالركن المادي والركن المعنوي

للجرائم الواقعة على أمن الدولة المعلوماتي، كالتوسع في تجريم مجرد التعريض للخطر، والتوسع في تجريم الشروع في التحريض.

الخاتمة

في نهاية هذا البحث يمكن القول أن موضوع جرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة موضوع شائك ومرتبط بمجال يعرف تطوراً سريعًا يمس كرامة الأشخاص، وينعكس أيضًا بلا شك سلبًا على حقوقهم، وينتقل من تهديد كيان الأمر في بعض الحالات إلى المعاملات الاقتصادية لكبريات الدول، فالجرائم المستحدثة عمومًا والجرائم محل الدراسة على وجه الخصوص أصبحت تكلف الدول خسائر مادية مرتفعة.

ولا شك أن متطلبات العدالة الجنائية تفرض على الأجهزة الحكومية بشكل عام، والأجهزة المسؤولة عن تتبع الجرائم وضبطها والتحقيق فيها بشكل خاص أن تتحمل مسؤولياتها نحو اكتشاف المجرمين وضبطهم ومحاكمتهم، ومثل هذا الأمر يقتضي توفير الإمكانات التقنية اللازمة، سواء في عملية التحقيق أو الكشف والاستدلال عن الجرائم، لاسيما بعد أن تطورت ليس فقط أساليب الكشف عن الجرائم، وإنما أيضًا تطور أساليب ارتكاب الجرائم، وظهور أنماط جديدة من الجرائم ما كانت التشريعات لتعرفها من قبل، إلا بعد أن ظهرت وسائل متطورة تمكن المجرمين ارتكاب جرائمهم بأساليب وطرق غير معهودةً.

وتنهض جرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة على ركن مادي وآخر معنوي، فأما الركن المادي، فهو سلوك يتخذ أحد صورتين الأولى: الاختراق أو مجرد الدخول لموقع أو بريد أو حساب خاص للدولة، والاختراق يعني الدخول غير المرخص به، أو المحال لأحكام الترخيص، أو الدخول بأي طريقة غير مشروعة، إلى نظام معلوماتي أو حاسب إلى أو شبكة معلوماتية، وما في حكمها. أما الدخول فيعني مجرد ولوج الموقع أو البريد الإلكتروني أو الحساب، فإن اتخذ السلوك المادي صورة الدخول وجب أن يكون عمديًا. فالجريمة لا تقع بالإهمال، ولكن إن تم الدخول عن طريق الخطأ ولم يتم مغادرة الموقع أو البريد الإلكتروني أو الحساب فوراً تحققت الجريمة.

ولقد اعتبر المشرع المصري في حكم الدخول المجرم تجاوز الحق فيه، فقد يكون الدخول مسموح به لشخص، ولكن في حدود زمن معين، أو على موقع دون حساب أو العكس فيخالف ذلك فتتحقق الجريمة، والصورة الثانية للسلوك الإجرامي هو اعتراض البيانات والمعلومات الحكومية أو الحصول عليها متى كانت تلك البيانات والمعلومات سرية، والاعتراض هنا يعني مشاهدة البيانات أو المعلومات أو الحصول عليها بغرض التنصت أو التعطيل أو التخزين أو النسخ أو التسجيل أو تغيير المحتوى أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه.

أما الركن المعنوي فيتخذ صوره القصد الجنائي بأن تتجه إرادة الجاني إلى السلوك مع العلم بكافة عناصر الركن المادي فإن أعوزه العلم لم يقم القصد، ولا يختلف الأمر عند دخول الموقع أو البريد الإلكتروني أو الحساب بطريق الخطأ إذ مكوث المتهم في الموقع أو البريد الإلكتروني أو الحساب وعدم المغادرة يحقق العلم لديه بأنه يعتدي على حسابات الدولة ومواقعها عبر شبكة الإنترنت.

أولًا: نتائج البحث:

١. سعا المشرعين المصري والعماني إلى تجريم أفعال الاعتداء أو التعدي على البيانات والمعلومات وكافة النظم المعلوماتية الخاصة بالدولة، سواء أخذ هذا التعدي شكل الدخول أو البقاء غير المشروع للنظام المعلوماتي، أو الإتلاف أو التعطيل أو تعديل مسار أو الإلغاء سواء كان كليًا أم جزئيًا، وذلك من أجل توفير نوع من الحماية اللازمة لجميع وسائل وأنظمة التقنية المعلوماتية الخاصة بالدولة من شبكات سلكية ولاسلكية وأجهزة ومعدات وبيانات وبرامج، وكذلك المعلومات المخزنة أو المعالجة أو المولدة أو المخلقة على أي نظام معلوماتي خاص بالدولة، وما في حكمه.

٢. جرم المشرع المصري والتشريعات المقارنة مجرد الدخول غير المشروع أو غير المصرح به إلى الموقع الإلكتروني، أو النظام الإلكتروني، أو الشبكة الإلكترونية، حيث يُعتبر الدخول غير المصرح به للنظام أو الشبكة الإلكترونية يُعتبر جريمة يُعاقب عليها التشريعات المقارنة.

٣. إن المصلحة الجديرة بالحماية فيما يتعلق بالجرائم محل البحث– والتي من أجلها أسبغ المشرع صفة التجريم والعقاب على كل سلوك ينطوي على تعريض مصالح الدولة وأمنها ونظامها المعلوماتي للخطر–تتمثل في حماية النظام السياسي للدولة، والحفاظ على وجودها وبقائها، وأمنها، وسلطاتها، وكذلك الحفاظ على كيانها الاجتماعي والاقتصادي.

٤. أفرد المشرع المصري لجريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة نصًا مستقلًا بخلاف المشرع العُماني والتشريعات المقارنة التي نصت على عدة صور يمكن اعتبارها أنماطًا للجرائم الواقعة على الأنظمة المعلوماتية الخاصة بالدولة، ويمكن حصر هذه الصور التجريمية في جريمة الدخول غير المشروع إلى النظام المعلوماتي، وكذلك جريمة التجسس المعلوماتي وجريمة الإتلاف والتدمير المعلوماتي، ولكل جريمة منها أحكامها التجريمية والعقابية الخاصة بها.

ثانيًا: توصيات البحث:

١. يُعتبر المشرع المصري موفقًا في الصياغة التشريعية أكثر من التشريعات المقارنة، وذلك بإفراده نصًا خاصًا ومستقلًا للجريمة محل البحث تضمنته المادة ٢٠ من القانون رقم ١٧٥ لسنة ٢٠١٨م بخلاف المشرع العُماني والتشريعات المقارنة التي نصت عليها كعدة صور تضمنتها قوانين مكافحة جرائم تقنية المعلومات؛ لذلك يقترح الباحث أن تحذو هذه التشريعات حذو المشرع المصري، وذلك بتقنين هذه الجريمة ضمن قوانينها المعنية مثلما فعل المشرع المصري.

٢. ضرورة توحيد النصوص التجريمية للاعتداءات الماسة بالأنظمة المعلوماتية الخاصة بالدولة، وتقريب الاتجاهات القانونية في الدول المقارنة بما يتناسب وفكرة عالمية أنظمة المعلوماتية الخاصة بالدولة وجرائم الاعتداء عليها، وبما يسمح في ذات الوقت باستيعاب ما قد يُستحدث في هذا المجال من تطور تقني في هذا الأمر.

٣. نرى ضرورة اعتبار جرائم الاعتداء على الأنظمة المعلوماتية من الجرائم الواقعة على أسرار الدفاع، حيث إن محتوى الأنظمة المعلوماتية الخاصة بالدولة تشتمل على معلومات وخطط حربية وسياسية واقتصادية وصناعية، وكذلك مكاتبات ومحررات ووثائق ورسوم وخرائط وتصميمات وصور وغيرها من الأشياء التي يجب لمصلحة البلاد أن تبقى سرًا، أو لا ينبغي أن يعلمها إلا الأشخاص الذين لهم صفة في ذلك، والتي يجب لمصلحة البلاد أن تبقى سرًا على من عداهم، وبالتالي يمكن أن يحكم القاضي في جرائم الاعتداء على النظم المعلوماتية الخاصة بالدولة بالعقوبات المقررة للجرائم الواقعة على أسرار الدفاع الواردة في قانون العقوبات لا سيما وأن المشرع العُماني قد قرر العقوبة إذا ما حصل عليها الجاني بأي وسيلة.

٤. نقترح أن ينص كل من المشرع المصري والإماراتي والكويتي والسعودي على الطرد والإبعاد للأجنبي كما نص عليه المشرع العُماني، وذلك في حالة إدانته في جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة، باعتبار أن هذا الإجراء حق وواجب للدولة تلجأ إليه في حالة مخالفة الأجنبي للأحكام الواردة بمكافحة تقنية المعلومات، لا سيما وأن وجوده بعد ارتكابه لهذه الجريمة يُشكل خطرًا على النظام العام أو الأمن، خاصة وأن تلك الأنشطة تتعارض مع المصالح العليا للبلاد أو التي من شأنها المساس بالسلم الاجتماعي.

٥. يقترح الباحث على المشرع العُماني والتشريعات المقارنة أن تنظم مسألة التدابير والإجراءات التحفظية كما نظمها المشرع المصري، وذلك بتبني إجراء حجب المواقع الإلكترونية التي استُخدمت في ارتكاب الجريمة أو كانت مسرحًا لها، وكذلك المنع من السفر وترقب الوصول ضمن قوانينها العقابية في شأن مكافحة جرائم تقنية المعلومات.

٦. نظراً للقصور التشريعي الحاصل في عدم النص صراحة على مدى خضوع المكونات المنطقية للحاسب الآلي للتفتيش؛ فإنه يجب مراعاة إضافة عبارة" المعلومات والأنظمة الإلكترونية أو البيانات المخزنة في الحاسب الآلي والمعالجة بواسطته" في نصوص المرسوم آنف الذكر، وذلك حتى يمتد ضبط الأدلة المادية للحاسب الآلي ليشمل البيانات والمعلومات بمختلف أشكالها.

قائمة بأهم المراجع

أولًا: المراجع العامة:

١. د. أحمد شوقي عمر أبو خطوة، المبادئ العامة في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، ٢٠١٣م.

٢. د. أحمد فتحي سرور، الوسيط في قانون العقوبات، القسم الخاص، الطبعة الرابعة، دار النهضة العربية، القاهرة، ١٩٩١م.

٣. د. أشرف توفيق شمس الدين، شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة والعقوبة، طبعة خاصة لطلاب التعليم المفتوح بكلية لحقوق بجامعة بنها، دون دار نشر، ٢٠٠٩م.

٤. د. غنام محمد غنام، د. تامر محمد صالح، شرح قانون العقوبات: القسم العام، بدون دار نشر، ٢٠٢٢م/٢٠٢٣م.

٥. د. محمد محرم محمد ود. خالد محمد المهيري، قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة فقهًا وقضاءً، الطبعة الثانية، الفتح للطباعة والنشر، الإسكندرية، ١٩٩٢م.

٦. د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، ١٩٩٢م.

٧. د. هدى حامد قشقوش، السياسة الجنائية لمواجهة الجريمة المعلوماتية، دار النهضة العربية، القاهرة، ٢٠١٢م.

ثانيًا: المراجع المتخصصة:

١.د. أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، ط١، دار النهضة العربية، القاهرة، ٢٠١٠م.

٢.. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، ١٩٩٢م.

٣.د. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت: دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٠٩م.

٤.د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٣م.

- النظام القانوني لحماية التجارة الإلكترونية، الطبعة الأولى، دار الفكر الجامعي الإسكندرية، الإسكندرية، ٢٠٠٢م.

٥.د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، بهجان للطباعة والتجليد، مصر، ٢٠٠٩م.
٦.د. عفيفي كامل عفيفي، جرائم الكمبيوتر، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت- لبنان، ٢٠٠٣م.
٧.د. عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، "الأحكام الموضوعية والأحكام الإجرائية"، دار النهضة العربية – القاهرة، ٢٠١٤م.
٨.د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، ٢٠٠١م.
٩.د. مدحت محمد عبد العزيز إبراهيم، الجرائم المعلوماتية الواقعة على النظام المعلوماتي: دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠١٥م.
١٠.د. محمود أحمد طه، المواجهة التشريعية والإنترنت: دراسة مقارنة، دار الفكر والقانون، المنصورة، ٢٠١٧م.
١١.د. ممدوح عبد الحميد عبد المطلب، جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية، مكتبة دار الحقوق، الشارقة، دولة الإمارات العربية المتحدة، ٢٠٠١م.
١٢.د. نائلة قورة، جرائم الحاسب الاقتصادية، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٠٤م.

ثالثًا: الرسائل الجامعية:

١. د.سالم بن مبارك بن سليم اليعقوبي، الحماية الجنائية للأدلة المعلوماتية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ١٤٤٠ه/٢٠١٩م.
٢. د. شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، ٢٠٠٥م.
٣. قصي أيمن البداودة، المسؤولية الجزائية الناشئة عن نشر وثائق الدولة عبر المواقع الإلكترونية، رسالة ماجستير، كلية الحقوق، جامعة الإسراء الخاصة، الأردن، ٢٠١٩م.
٤. نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية، ٢٠٠٦م
٥. د. نور سليمان يوسف يعقوب البالول، الأحكام الموضوعية لجرائم المعلوماتية: دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ١٤٤٢ه/٢٠٢١م.

٦. د. يوسف بن سعيد بن محمد الكلباني، الحماية الجزائية للبيانات الإلكترونية في التشريعين العماني والمصري، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق–جامعة عين شمس، ١٤٣٧هـ/٢٠١٦م.

رابعاً: البحوث والدراسات والمؤتمرات:

١. د. أشرف محمد نجيب السعيد الدريني، جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات: دراسة تحليلية مقارنة، بحث منشور في مجلة روح القوانين، كلية الحقوق، جامعة طنطا، المجلد ٩٥، العدد ٩٥، يوليو ٢٠٢١م.

٢. د. عبد الإله محمد النوايسة، جرائم التجسس الإلكتروني في التشريع الأردني: دراسة تحليلية، مجلة دراسات–علوم الشريعة والقانون، عمادة البحث العلمي، الجامعة الأردنية، المجلد ٤٦، ملحق، ٢٠١٩م.

- جريمة الدخول غير المشروع في تشريعات الجرائم الإلكترونية العربية: دراسة مقارنة، المجلة القانونية والقضائية، السنة (١٠)، العدد (١)، ٢٠١٦م.
- دور قانون مكافحة الجرائم الإرهابية الإماراتي في مكافحة الخطورة الإجرامية في جرائم الإرهاب، مجلة جامعة الشارقة للعلوم القانونية، المجلد ١٥، العدد ١، رمضان ١٤٣٩هـ/ يونيو ٢٠١٨م.

٣. د. عبد الإله محمد النوايسة وآخرين، جرائم التجسس الإلكتروني في التشريع الأردني: دراسة تحليلية، مجلة دراسات–علوم الشريعة والقانون، عمادة البحث العلمي، الجامعة الأردنية، المجلد ٤٦، ملحق، ٢٠١٩م.

٤. د. محمد نصر محمد عوض القطري، الإشكاليات القانونية لحماية سلامة المعلومات: دراسة تطبيقية على الحماية الجنائية من الإتلاف المعلوماتي، بحث منشور في مجلة الفكر الشرطي، القيادة العامة لشرطة الشارقة، مركز بحوث الشرطة، دولة الإمارات العربية المتحدة، المجلد ٢٤، العدد ٩٣، أبريل ٢٠١٥م.

٥. . لورنس سعيد أحمد الحوامدة، الجرائم المعلوماتية: أركانها وآلية مكافحتها: دراسة تحليلية مقارنة، مجلة الميزان للدراسات الإسلامية والقانونية، جامعة العلوم الإسلامية العالمية، عمان، الأردن، المجلد ٤، العدد١، يناير ٢٠١٧م.

٦. د. هدى حامد قشقوش، الإتلاف العمدي لبرامج وبيانات الحاسب الإلكتروني، بحث مُقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، دولة الإمارات، الفترة من ١: ٣ مايو ٢٠٠٠م.

- جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي في الفترة ٢٥–٢٨ أكتوبر ١٩٩٣م.

٧. د. هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني واقتراح بإنشـــاء آلية عربية موحدة للتدريب التخصصي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنـــت الذي نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، ٢٠٠٠م.

خامسًا: المراجع باللغة الفرسية:

1. AGSOUS Naima," cybercriminalite : les reseaux informatiques revue de la gendarmerie , N29 November, 2008.
2. Francois Debrix,"Tabloid Terror:War, Culture, and Geopolitics",Published by Routledge, London, U.K., 2008.
3. Roland Drago et Jean-Marie Auby,"Traité de contentieux administratif",Librairie générale de droit et de jurisprudence impr. R. Vançon , 1962.
4. Stephane Debray,"Internet face aux substances illicites",complice de la cybercriminalité ou outil de prévention ?, DESS média électronique & Internet de l'Université de Paris 8, Année académique 2002-2003.
5. Sevgi Kelci,"Vol, fraude et autres infractions semblables et Internet",Revue Lex Electronica , Vol.12,n°1 ,2007, P.7, disponible sur le site: http://www.lex-electronica.org/articles/v12-1/kelci.pdf Consulté le 12/01/2022 à 11h30.
6. Melanie Kowalski,"Cybercriminalité : enjeux, sources de données et faisabilité de recueillir des données auprès de la police", Centre canadien de la statistique juridique,No 85-558-XIF au catalogue,Décembre 2002,Consulté le 05/11/2021 à 13h15, https://www150.statcan.gc.ca/n1/fr/pub/85-558-x/85-558-x2002001-fra.pdf?st=IXUiSy_b

سادسًا: المراجع باللغة الإنجليزية:

1. Behrouz A. Forouzan,"Introduction to cryptography and network security",Cryptography and network security",Publisher by New York, NY : McGraw-Hill Higher Education, 2008.
2. Bainbridge. D: Introduction to computer law, fourth edition, London, 2000.
3. Eric J. Sinrod, and William P Reilly, "Cyber- Crimes: A practical approach to the Application of Federal Computer Crimes Laws, 16 Santa Clara computer and High Tech L. J. 177, P.90, (2000).
4. David Emm and Others,"IT threat evolution in Q2 2016. Statistics", Kaspersky Lab detected, 11 AUG 2016, P.12. on the following website: https://securelist.com/it-threat-evolution-in-q2-2016-statistics/75640/,Accessed 25/12/2022 at 01.15 Pm.
5. David Febrache, Pathology of computer viruses, Springs Overlay, New York, 1992.
6. Tim Maurer,"WikiLeaks 2010: A Glimpse of the Future?",Science, Technology, and Public Policy Program Explorations in Cyber International Relations Project,Belfer Center for Science and International Affairs,Harvard Kennedy School,Cambridge, USA, 2011.

13. Walter Gary Sharp, Redefining National Security in Today's World of information technology and Emergent Threats, 9 Doke J Comp and Int'l,1999.