كلية الحـــــــــــــقوق

الدراســــــــــــات العليـــــــا

قسم القانون الجنائي

مفهوم جريمة اختراق المواقع الإلكترونية الرسمية وأساسها القانوني

(دراسة مقارنة)

بحث مستل من رسالة لنيل درجة الدكتوراة في الحقوق

تحت إشراف

الأستاذ الدكتور : أكمل يوسف السعيد

الأستاذ المساعد بقسم القانون الجنائي

إعداد الباحث

خليفه عبيد جمعه سلمون الصريدي

مفهوم جريمة اختراق المواقع الإلكترونية الرسمية وأساسها القانوني (دراسة مقارنة

المقدمة

أولًا – التعريف بموضوع الدراسة: الجريمة بوجه عام ليست بجديدة في عالم البشر، وإنما هي موجودة بوجود الإنسان على سطح المعمورة، وذلك منذ أن قتل قابيل هابيل، ثم تطورت الجريمة بتطور المجتمع؛ فظهرت جرائم وأساليب لم تكن موجودة في السابق، وهو ما أوجب على القائمين بمكافحة الجرائم تحديث الأنظمة والقوانين والإجراءات، وتطويرها لمواجهة المستحدث منها.

وقد شهد العالم أجمع تطوراً هائلًا في جميع مجالات الحياة، ولعل أهم ما أفرزه هذا التطور ظهور ما يعرف بالحاسب الآلي؛ حيث إنه أصبح بالنسبة للمجتمع مصدراً هامًا ووسيلة لا يمكن الاستغناء عنها بحال من الأحوال، فلا تجد مكانًا إلا والحاسب الآلي يستخدم فيه بأحد أشكاله العديدة، سواء أكانت حواسيب مكتبية، أم حواسيب محمولة، أم أجهزة هواتف محمولة، تعتمد على برامج تشغيل موحدة للحواسب الآلية ضمن شبكة تربط العالم بأسره، وتسمى شبكة المعلومات الدولية (الإنترنت)، وهي شأنها شأن أيّ اختراع حديث قد ظهر، لها ما لها من الإيجابيات، وعليها ما عليها من السلبيات، ومن سلبياتها ما يعرف باختراق المواقع الحكومية الرسمية، والعبث بما تضمنه تلك المواقع من البيانات والمعلومات، وهو ما يمثل اعتداءً على أمن الدولة، ومن ثم يعاقب قانون الجرائم المعلوماتية كل من يخترق المواقع الحكومية الرسمية، ولا تجوز هذه الأفعال خلقًا ولا قيمًا، كما تهدف ممارسة هذه الأفعال إلى بث الرعب والذعر والخوف والهلع بين أفراد المجتمع، وإثارة الفتن بين طوائفه، بما تمثله من الاعتداء على خصوصيات الدولة.

ثانيًا – أهمية الدراسة: إنّ استخدام شبكة الإنترنت بشكل كبير، وانتشارها الواسع في الآونة الأخيرة في جميع دول العالم – ومن ضمنها الدول العربية والإسلامية – صاحبه ظهور العديد من السلبيات والإيجابيات، سواء على المستوى الأمني، أم الاجتماعي، أم الثقافي، أم الاقتصادي، أم السياسي، بالإضافة إلى الكثير من المشاكل القانونية، ناهيك عن تطور الأنشطة الإجرامية.

وقد أظهر التحليل الشامل للشكاوي المقدمة إلى تقارير مركز شكاوى احتيال الإنترنت الأمريكي **(IFFC)**، قد بينت أنّ عدد البلاغات الواردة إلى المركز خلال نصف عام فقط من بداية أعمال المركز قد بلغت (٦٠٨٧) شكوى، من بينها (٥٢٧٣) حالة مرتبطة بالحاسب الآلي عبر شبكة الإنترنت[١].

---

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

ثالثًا – مشكلة الدراسة: دعت الحاجة إلى هذه الدراسة، والتي تعتمد على فرضيات ثابتة، وهي أن اختراق المواقع الإلكترونية الحكومية يمثل تهديداً حقيقياً لكافة ما تبنيه الدولة في العصر الحديث، وما يسفر عنها من المعلومات والبيانات والشبكات والحكومات الإلكترونية، وكذلك محاولة تدمير محطات توليد الطاقة وتنقية المياه ووسائل الاتصالات والمواصلات وشركات الطيران والمؤسسات المالية والاقتصادية، إذ أن جميع هذه المصالح والهيئات لا تتمتع بحصانة حقيقية لبناها التحتية في أي قانون أو تشريع في أي دولة، ومن ثم عجزها وعدم قدرتها على مواجهة مثل هذا النوع من الاختراق الحديث، ومن ثم يجب التأكيد على ضرورة التعرف على ظاهرة اختراق المواقع الإلكترونية الحكومية، ووسائل تهديداتها، بقصد الوصول إلى وضع اقتراحات لتحديد آليات التصدي والمواجهة للحد من مخاطر اختراق المواقع الإلكترونية الحكومية، ومن ذلك يمكن تحديد مشكلة الدراسة في التساؤل التالي: ما هو الاختراق الإلكتروني لمواقع الحكومية الرسمية؟ ودور المشرع – الإماراتي والمصري – في مكافحته والتصدي له؛ حيث أخذت هذه الظاهرة في الانتشار على نطاق واسع، على نحو أثار معه قلق العلماء والدارسين والباحثين في التصدي لهذه المشكلة.

رابعًا – منهج الدراسة: أما المنهج الذي ساستخدمه في هذه الدراسة فهو المنهج الوصفي التحليلي، والذي يقوم على تشخيص الواقع، ومعرفة الأسباب الفعلية لتكون جريمة الاختراق للمواقع الرسمية الحكومية، ومدى كفاية النصوص التشريعية في مواجهتها، وكذلك المنهج المقارن؛ حيث نتبع في هذه الدراسة مقارنة التشريع المصري والإماراتي باعتبارهما نظام واحد، نقارنهما بالنظام اللاتيني أو الآنجلو أمريكي، وبيان ما بينهما من أوجه اتفاق واختلاف.

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

المبحث الأول: ماهية جريمة اختراق المواقع الرسمية.

المبحث الثاني: الأساس القانوني لجريمة اختراق المواقع الرسمية غي القوانين الإماراتية والمقارنة

المبحث الأول

ماهية جريمة اختراق المواقع الرسمية

وقد شهد العالم أجمع تطوراً هائلًا في جميع مجالات الحياة، ولعل أهم ما أفرزه هذا التطور ظهور ما يعرف بالحاسب الآلي؛ حيث إنه أصبح بالنسبة للمجتمع مصدراً هامًا ووسيلة لا يمكن الاستغناء عنها

بحال من الأحوال، فلا تجد مكاناً إلا والحاسب الآلي يستخدم فيه بأحد أشكاله العديدة، سواء أكانت حواسيب مكتبية، أم حواسيب محمولة، أم أجهزة هواتف محمولة، تعتمد على برامج تشغيل موحدة للحواسب الآلية ضمن شبكة تربط العالم بأسره، وتسمى شبكة المعلومات الدولية (الإنترنت)، وهي شأنها شأن أيّ اختراع حديث قد ظهر، لها ما لها من الإيجابيات، وعليها ما عليها من السلبيات، ومن سلبياتها ما يعرف باختراق المواقع الحكومية الرسمية، والعبث بما تضمنه تلك المواقع من البيانات والمعلومات، وهو ما يمثل اعتداءً على أمن الدولة، ومن ثم يعاقب قانون الجرائم المعلوماتية كل من يخترق المواقع الحكومية الرسمية، ولا تجوز هذه الأفعال خلقًا ولا قيماً، كما تهدف ممارسة هذه الأفعال إلى بث الرعب والذعر والخوف والهلع بين أفراد المجتمع، وإثارة الفتن بين طوائفه، بما تمثله من الاعتداء على خصوصيات الدولة.

وعلى الرغم من التقدم التقني في مجال نقل المعلومات وتداولها، واتجاه عدد من الدول إلى الحكومة الإلكترونية، إلا أن إساءة استخدام التكنولوجيا شكلت تهديداً لخصوصية الحكومات، واعتداء على أسرارها بالعبث والتخريب تارة، وتسريبها ونشرها تارة أخرى، من خلال الاعتداء على المواقع الرسمية للدول.

ولما لم تكن بلادنا بدعًا بين هذه الدول، فقد تعرضت مواقعها الإلكترونية الرسمية للاختراق والاقتحام، فقد ظهرت في الآونة الأخيرة العديد من جرائم الاختراق للمواقع الإلكترونية الرسمية في دولة الإمارات العربية ومصر وغيرهما من الدول العربية، ولما كانت هجمات القراصنة الإلكترونيين على المواقع الحكومية في الدولة تزداد يوم بعد يوم، **فإننا نرى:** ضرورة الحاجة لبيان حدود المسؤولية الجنائية عن هذا النوع من الاختراقات، والعقوبات المقررة له، وذلك من خلال دراسة نصوص القانون الإماراتي ومقارنتها بنصوص القانون المصري.**كما أن** استخدام شبكة الإنترنت بشكل كبير، وانتشارها الواسع في الآونة الأخيرة في جميع دول العالم – ومن ضمنها الدول العربية والإسلامية – صاحبه ظهور العديد من السلبيات والإيجابيات، سواء على المستوى الأمني، أم الاجتماعي، أم الثقافي، أم الاقتصادي، أم السياسي، بالإضافة إلى الكثير من المشاكل القانونية، ناهيك عن تطور الأنشطة الإجرامية، وقد أظهر التحليل الشامل للشكاوي المقدمة إلى تقارير مركز شكاوى احتيال الإنترنت الأمريكي **(IFFC)**، قد بينت أنّ عدد البلاغات الواردة إلى المركز خلال نصف عام فقط من بداية أعمال المركز قد بلغت (٦٠٨٧) شكوى، من بينها (٥٢٧٣) حالة مرتبطة بالحاسب الآلي عبر شبكة الإنترنت[١].

(١) حسين بن سعيد الغافري، السياسة الجنائية في مواجهة الإنترنت – دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٩م، ص٩.

وتعد الظاهرة الإجرامية ملازمة للمجتمع الإنساني، وتعكس في أساليبها وأنماطها أحوال وتطورات المجتمع في مختلف النواحي السياسية والاقتصادية والاجتماعية والثقافية. فشهد العالم خلال الربع الأخير من القرن الماضي تحديات كبيرة ومتزايدة نتيجة التطور السريع في الميدان العلمي والتكنولوجي حيث أصبح جهاز الكمبيوتر ركيزة أساسية في عصرنا وتطور دوره بحيث تعدى إجراء العمليات الحسابية المعقدة ليشمل قضايا في شتى مجالات الحياة المختلفة وبات هناك ظهور أنواع جديدة من الجرائم تختلف في محلها وأسلوب ارتكابها عن الجرائم التقليدية، فوظف المجرمون هذه المبتكرات التقنية في تطوير أساليبهم الإجرامية والحصول على أية معلومات بسرعة فائقة وبدون صعوبات مما جعل العالم بمثابة قرية صغيرة لا يعترف للحدود الجغرافية بمعنى ذوبانها وذلك عن طريق وسائل الاتصال الفورية على الأرض، أو من خلال الفضاء لتضيف بعداً كبيراً لقدرة المجرم على توسيع معرفته وتخزينه وإنتاج المعلومات والبث لها وتبادل الصفقات[٢]، فأصبح الخطر يتزايد شيئًا فشيئًا، مما ظهر صوراً جديدة من الإجرام ارتبطت بهذه التقنيات كمحل أو وسيلة لها، كما ضاقت نصوص القوانين العقابية عن استيعاب هذا النوع من الجرائم، فلم تكن القوانين الإجرائية أفضل حظًا منها سيما أنها أمام جرائم ترتكب قد يفلت مرتكبيها من العقاب مما يلحق أشد الضرر بالمجتمع، وبالأفراد، فشكلت تحدياً كبيراً للفقه والتشريع والقضاء ذلك أن مرتكبي هذه الجرائم يتسمون بالذكاء والخبرة في التعامل في مجال المعالجة الآلية للمعطيات والإلمام بالمهارات والمعارف التقنية، ومن هنا برزت خطورة الجرائم الإلكترونية في سهولة ارتكابها وصعوبة تتبع مرتكبيها مما يستدعي أخذ الحيطة ووضع آلية للتعامل مع هذه الجرائم، وفي ضوء من تقدم، فإننا نتناول في هذا الفصل ماهية جريمة اختراق المواقع الإلكترونية الرسمية للدولة، وذلك من خلال ثلاثة مطالب على النحو الآتي:

المطلب الأول: تعريف جريمة اختراق المواقع الإلكترونية الرسمية للدولة.

المطلب الثاني: خصائص جريمة اختراق المواقع الإلكترونية الرسمية للدولة.

المطلب الثالث: صور جريمة اختراق المواقع الإلكترونية الرسمية للدولة.

المطلب الثاني

تعريف جريمة اختراق المواقع الإلكترونية الرسمية للدولة في القانون

اختراق المواقع الرسمية للدولة: هو حالة الدخول غير المشروع إلى مواقع إلكترونية أو نظام معلوماتي بطريقة مباشرة عن طريق شبكة المعلومات الدولية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات ومعلومات ماسة بالأمن الداخلي أو الخارجي للبلاد، ومن ثم العبث بأمنها واستقرارها

---

(٢) محمد سيد محمد، وسائل الإعلام من المنادي إلى الإنترنت، دار الفكر العربي، القاهرة، ٢٠٠٩م، ص١٦.

واقتصادها القومي[٣]، وكذلك فإن الدخول غير المشروع إلى البيانات بقصد العبث أو التطفل، أو بهدف ارتكاب أو تسهيل ارتكاب أفعال أخرى، أو تعديلها أو تحويرها، أو إضعاف أو تعطيل النظام.

وإذا كان من الصعوبة بمكان وضع تعريف دقيق لأي مصطلح قانوني بصفة عامة، فإن ذلك ينطبق – بصفة خاصة – علي تعريف الجريمة الإلكترونية، حتى ردد البعض معبراً عن هذه الصعوبة، بأن الجريمة المعلوماتية تقاوم التعريف، أو أنها فوق مستوى التعريف، أو أنها صعبة التعريف، ويقول الأستاذ Devéze "أن المقصود وضع مفهوم إجرامي أكثر من مجرد وضع وصف قانوني؛ لأن المفهوم الإجرامي سيكون عبثًا أن يطبق عليه أحد التعاريف المقول بها ماليًا أو مدنيًا أو جنائيًا"[٤]، بينما يري الأستاذ Trédemann "أن الجريمة المعلوماتية هي تلك التي تشمل أي جريمة ضد المال عن طريق استخدام المعالجة الآلية للمعلومات"[٥]. كما يعّرف البعض الجريمة الإلكترونية بأنها "فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه"[٦]، كما عرفت بأنها: "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية لازمًا بقدر كبير لارتكابه من ناحية، ولملاحقته وتحقيقه من ناحية أخري"[٧]،

الجريمة التقليدية رغم ما عرفته من جدل بين الفقهاء حول تعريفها إلا انه اتفق على تعريفها:" بالفعل غير المشروع الصادر عن ارادة جنائية يقرر لها القانون عقوبة، وتدبيراً احترازياً"[٨] اما الجريمة الاكترونية فنجد الفقه لم يُجمع على وضع تعريف جامع لها فتعددت التعريفات الفقهية مما دفعهم للقول إنها جريمة تقاوم التعريف او انها الجريمة المانعه[٩] واختلفت الاتجاهات الفقهية في تعريفها حول المعيار الواجب الاعتماد عليه مما آثار ذلك العديد من المشاكل العملية المتمثلة بصعوبة تقدير حجم

---

(٣) مصطفى محمد موسى، الإرهاب الإلكتروني، دراسة (قانونية – أمنية – نفسية – اجتماعية) ط١، سلسلة اللواء الأمنية في مكافحة الجرائم الإلكترونية،١٤٣٠هـ/٢٠٠٩م، ص١١٢.

(4) J. Devéze , Les Qualifications Penalesaux Fraudes informatiques , in Le droit Criminel Face au techniques de communication lieés à l'informatique p. 186 .

(5) K. Tiedemnn , Fraude et autres délits d'afaires commis à l'aide d'ordinateurs électroniques ,Rev. droit penal crim. 1984 p. 612 .

(6) Schiolberg (s) – Computers and penal Leg is Lation, as tudy of the Legal politics of a new technology ,1983, p4 .

(6) Chen – christopher D. Computer Crime , The Computer Fraud and Abuse act of 1986 , C.L.J... 1990 , Vol 10 , p.72

(٧) محمود نجيب حسني، شرح قانون العقوبات القسم العام، دار النهضه العربية، القاهره، ٢٠١٦م، ص١٠٤.

(٨) هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤م، ص٢٩.

(٩) نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، دار النهضة العربية، القاهرة، ٢٠٠٤م، ص٢٥.

المخاطر التي تسببها هذه الجرائم من جانب وفي تعذر الحلول لمواجهتها وصعوبة تحقيق تعاون دولي لمكافحتها في جانب آخر منه[١٠].

فاستند الفقهاء في تعريف الجريمة الإلكترونية إلى مفاهيم متعددة وحددوا عدداً ليس بالقليل من التعريفات تتباين وتتمايز بينها فمنهم من عرفها على أساس وسيلة ارتكابها (الكمبيوتر) ومنهم من عرفها على أساس الغاية ومنهم من عرفها استنادا لمعيار شخص الفاعل الذي يتطلب أن يكون ملماً بتنقية المعلومات ومنهم من عرفها استناداً لموضوع الجريمة وهناك من دمج التعريفات في تعريف واحد وهذا الخلاف يمكن ان نبينه في النقاط الاتية:

اولًا – تعريف جريمة اختراق المواقع الإلكترونية الرسمية للدولة بالنظر إلى وسيلة ارتكابها (الحاسب الآتي):

استناداً لهذا المعيار يرى جانب من الفقه في تعريفهم للجريمة الإلكترونية على أساس وسيلة ارتكابها المتمثلة بجهاز الحاسوب أو الكمبيوتر أو إحدى وسائل التقنية الحديثة المرتبطة به فتعد الجريمة الإلكترونية متى كان جهاز الحاسب الآلي أو الكمبيوتر وسيلة لارتكابها.

فعرفها الفقيه Merwe بأنها: "الفعل غير المشروع الذي يتورط بارتكابه الكمبيوتر"[١١]، أو أنها: "كل فعل أو امتناع عمدي ينشأ عن نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة في الكمبيوتر أو التي تحول عن طريقه"[١٢]، وكما عرفها أخر أنها: "كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب عن طريق الكمبيوتر وداخلًا بارتكابها"[١٣]، وعرفها جانب آخر من الفقه على أنها: "كل سلوك غير مشروع أو مناف للأخلاق أو غير مسموح به يرتبط بالمعالجة الآلية للبيانات أو بنقلها"[١٤]، وفي نفس الاتجاه وعرفها الفقيهان Michel & Credo على " إنها سوء استخدام الكمبيوتر أو جريمة الكمبيوتر والتي تسهل استخدام الكمبيوتر كأداة ارتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به بجهاز كمبيوتر المجني عليه أو بياناته[١٥]، وفي ذات

---

(١١) محمد أمين الشوابكة، جرائم الحاسوب والإنترنت الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان – الأردن، ٢٠١٥م، ص٨.

(١٢) لورنس حوامدة، الجرائم المعلوماتية وأركانها وآلية مكافحتها – دراسة تحليلية مقارنة، بحث منشور في مجلة الميزان للدراسات الإسلامية والقانونية، جامعة العلوم الإسلامية، المجلد الرابع، العدد الأول، كانون الثاني، ٢٠١٧م، ص١٨٨.

(١٣) هشام محمد فريد رستم، الجرائم المعلوماتية أصول التحقيق الجنائي الفني، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ٢٠٠٠م، ص٨، بحوث مؤتمر القانون والكمبيوتر والإنترنت، المجلد الثاني، ط٣، جامعة الإمارات العربية المتحدة، ٢٠٠٤، ص٤٠٥.

(١٤) علي عبد القادر القهوجي، الحماية الجنائية لجرائم الحاسب، بحث منشور بمجلة الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية، العدد ٢٤، ١٩٩٢م، ص١٧٢.

(١٥) هلالي عبد اللاه أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية – دراسة مقارنة، دار النهضة العربية، القاهرة، ١٩٩٧م، ص١٤.

النص يرى الفقيهان Richard totty وAnthony Flardcastle بأنها" تلك الجرائم التي يكون قد وقع في مراحل ارتكابها بعض عمليات فعلية داخل نظام الكمبيوتر والتي يكون له دورا فيها إيجابي أكثر من أنه سلبي[١٦] ويتضح من مدول التعريفات السابقه انها تركز على الوسيلة المستخدمة بواسطة جهاز الكمبيوتر دون الجرائم الواقعة على الكمبيوتر بحسب سلوك الجاني وجميع أنواع محل الجريمة[١٧]، فجاءت قاصرة عن تحديد الغاية أو الهدف من السلوك غير المشروع فالمشرع عند تجريمه السلوك لا ينظر إلى الوسيلة أو الأداة المستخدمة.

ثانيًا – تعريف جريمة اختراق المواقع الإلكترونية الرسمية للدولة بالنظر إلى غايتها:

وفي هذا المعيار يرى جانب من الفقه بتعريفهم للجريمة الإلكترونية انه يستند إلى الغاية التي يراد في تحقيقها أو ما تنتج عنها مع عدم حصر الجريمة في جهاز الكمبيوتر وحده وإنما بالتقنية المستخدمة في كافة الأجهزة المعلوماتية، وعرفت وفق هذا المعيار على أنها: "كل فعل إجرامي متعمد أيًا كانت صلته بالمعلوماتية ينشأ عنه خسارة المجني عليه أو كسبًا يحققه الفاعل[١٨]، أو هي كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات ويهدف إلى الاعتداء على الأموال والحقوق المعنوية"[١٩]، أو أنها كل سلوك غير معاقب عليه قانونًا صادر عن إرادة مذنبة ومحله معطيات الكمبيوتر[٢٠]. فيرى الفقيه الفرنسي Mass ان المقصود بالجريمة االلكترونية يتمثل باعتداءات غير مشروعة ترتكب بواسطة المعلوماتية بغرض تحقيق الربح[٢١]، ومما يدل بتركيز التعريفات على معيار الوسيلة والربح أي التي يستخدم الكمبيوتر في ارتكابها وتهدف إلى تحقيق مكسب مادي لذا يؤخذ على هذه التعريفات أنها عالجت أمر الجرائم الإلكترونية على حسب الغاية من الجريمة وبالتالي ضيق نطاقها وجعلها قاصرة على الجرائم الواقعة على الكمبيوتر أو معطياته دون الجرائم الواقعة بواسطته.

ثالثًا – تعريف جريمة اختراق المواقع الإلكترونية الرسمية للدولة بالنظر إلى شخصية الجاني: إذا كان من الصعب وضع تعريف دقيق لأي مصطلح قانوني بصفة عامة، فإن ذلك ينطبق – علي وجه الخصوص – علي تعريف الجريمة المعلوماتية ، حتى ردد البعض معبراً عن هذه الصعوبة بأن

---

(١٦) أيمن عبد الله فكري، جرائم أنظمة المعلومات، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٧م، ص٨٣.

(١٧) محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٤م، ص٣٤.

(١٨) محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، ط٢، دار النهضة العربية، القاهرة، ١٩٩٨م، ص٦.

(١٩) عبد الله حسين محمود، إجراءات جمع الأدلة في مجال سرقة المعلومات، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات المنعقد في الفترة ٢٦–٢٨ أبريل ٢٠٠٣م، دبي – الإمارات العربية المتحدة، ص٣.

(٢٠) نائل عبد الرحمن صالح، واقع جرائم الحاسوب في التشريع الأردني، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ٢٠٠٠م، ص٣.

(٢١) أيمن عبد الله فكري، جرائم نظم المعلومات، مرجع سابق، ص٩٠.

الجريمة المعلوماتية تقاوم التعريف،ويقول الأستاذ Devéze " أن المقصود وضع مفهوم إجرامي أكثر من مجرد وضع وصف قانوني ، لأن المفهوم الإجرامي سيكون عبثًا أن يطبق عليه أحد التعاريف المقول بها ماليًا أو مدنيًا أو جنائيًا "(٢٢).

ويري الأستاذ Trédemann " أن الجريمة المعلوماتية هي تلك التي تشمل أي جريمة ضد المال عن طريق استخدام المعالجة الآلية للمعلومات" (٢٣)، ويري الأستاذ Parker أن الجريمة المعلوماتية هي " كل فعل إجرامي متعمد – أيا كانت صلته بالمعلوماتية – ينشأ عنه خسارة تلحق المجني عليه أو كسب يحققه الفاعل" (٢٤)، ويري الأستاذ Masse أن الغش المعلوماتي هو "الاعتداءات القانونية التى ترتكب بواسطة المعلوماتية بغرض تحقيق ربح " (٢٥)، وهناك اتجاه في الفقه يذهب أنصاره إلي تضييق مفهوم الجريمة المعلوماتية يشترط في الفاعل أن يكون عالما بتكنولوجيا الحاسبات الآلية بقدر كبير لاعتبار جريمته معلوماتية فذهب إلي تعريفها بأنها " كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية لازمًا بقدر كبير لارتكابه من ناحية ، ولملاحقته وتحقيقه من ناحية أخري"(٢٦) ، وقد أخذت وزارة العدل الأمريكية بهذا التعريف في تقرير صادر عنها عام ١٩٨٩م يتعلق بجرائم المعلوماتية

يستند أصحاب هذا المعيار بتعريفهم للجرائم الإلكترونية إلى شخصية فاعلها(الجاني) الذي يتطلب منه معرفة تقنية بتكنولوجيا الكمبيوتر فهي تنصب على سمة من سمات الجاني(٢٧).فقد تبنى معهد ستانفورد في الولايات المتحدة الأمريكية في إحدى دراساته هذا المعيار حيث عرفته وزارة العدل الأمريكية بدليلها الصادر سنة ١٩٧٩ "في أنها جريمة لفاعلها معرفة فنية بتقنية الحاسبات تمكنه من ارتكابها"(٢٨)، كما عرفها الفقيه Stein Schiollbery البلجيكي أنها "الجرائم التي تتطلب إلماماً خاصاً بتقنيات

---

(22) J. Devéze , Les Qualifications Penalesaux Fraudes informatiques , in Le droit Criminel Face au techniques de communication lieés à l'informatique p. 186 .

(23) K. Tiedemnn , Fraude et autres délits d'afaires commis à l'aide d'ordinateurs électroniques ,Rev. droit penal crim. 1984 p. 612 .

(24) D.B. Parker , Combattre La Crimpinalité informatique , éd Oros : 1985,p.18.

(25) M.Masse. la droit pénal special né del'informatique et doit pénal , Travaux de l'institut de sciences criminelles de poietiers 1981– léd cujas p. 23 .

(26) Chen – christopher D. Computer Crime , The Computer Fraud and Abuse act of 1986 , C.L.J... 1990 , Vol 10 , p.72.

(٢٧) أحمد أسامة حسنية، الجريمة الإلكترونية بين الشرعية الجنائية والإجرائية، مجلة جامعة الأزهر، غزة، عدد خاص بمؤتمر كلية الحقوق الخامس، المحكم، المجلد ١٩، ٢٠١٧م، ص٦.

(٢٨) هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص٤٤؛ نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الإسكندرية ، ٢٠٠٨م، ص٥٩.

الكمبيوتر ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها"[٢٩]. وعرفت من آخرين على أنها "جريمة تقنية تنشأ في الخفاء يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية وتوجه للنيل من الحق في المعلومات وتعتدي على معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكة المعلومات"[٣٠] ويتضح من مدلول التعريفات انها تؤكد على ضرورة ان يكون لدى الجاني معرفة ودراية بتقنية وتكنولوجيا الكمبيوتر وان لا يتوافر لدي اجهزة التحقيق سواء سلطات جمع الاستدلالات او التحقيق الابتدائي الالمام بهذه التكنولوجيا ولذا انتقد الفقه اصحاب هذا المعيار بأنه تطلب بشخصية الفاعل توافر صفات كالمعرفة التقنية مما يؤدي ذلك بالبحث عن الظروف الخاصة بالجاني للوصول إلى حقيقة وجود مثل هذه المعرفة من عدمها وهذا لا يتناسب مع القانون الجنائي كونه قانون موضوعي لا يعتد بالظروف الشخصية للجاني إلا على سبيل الاستثناء ذلك أن هذه الجرائم يرتكبها جزء كبير من أشخاص تتوزع أدوارهم بين التخطيط والتنفيذ والتحريض[٣١] مما يجعلها تعريفات قاصره عن تعريف واضح لهذا النوع من الجرائم، وتعد فكرة استخدام آلة (كمبيوتر) في معالجة الأرقام ليست بالجديدة؛ حيث أشار بعض الباحثين إلي استخدام مثل هذه الوسيلة – في صورتها الأولي – وجد في آسيا منذ خمسة آلاف عام، كما أن التزايد في معدل الحوادث الإلكترونية ما هو إلا بسبب دخول الإنترنت، وعلي وجه الخصوص التحريض على الإرهاب عبر وسائل إلكترونية، وغير ذلك من الجرائم غير العمدية والتي تزايدت زيادة مضطردة[٣٢].

وفي الفترة التي تولى فيها بيل كلينتون الرئاسة، أجرت الإدارة الأمريكية عدة خطوات تنفيذية تهدف إلى مكافحة التحريض على الإرهاب عبر وسائل إلكترونية (Cyber terrorism)، وتطبيقًا لذلك تم إنشاء لجنة، أطلق عليها لجنة حماية البنية الحساسة (President'sCommission on Critical Infrastructure Protectio)، واختصاراً يرمز لها بالرمز (PCCIP)[٣٣].

ومن الجدير بالذكر ما يترتب على هذه الصور الإرهابية من خسائر مادية فادحة؛ حيث تتحمل الدول خسائر مالية كبيرة، قد تصل إلى مئات المليارات من الدولارات، وذلك كأثر لتزايد الجرائم المعلوماتية بوجه عام، وجرائم الإرهاب الإلكتروني بوجه خاص[٣٤].

---

(٢٩) عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دار الكتب القانونية، المحلة الكبرى، مصر، ٢٠٠٦م، ص٢٥.

(٣٠) عبد الله حسين محمود، إجراءات جمع الأدلة في مجال سرقة المعلومات، مرجع سابق، ص٥٨٩.

(٣١) أيمن عبد الله فكري، جرائم نظم المعلومات، مرجع سابق، ص٦٣؛ أحمد أسامة حسنية، الجريمة الإلكترونية بين الشرعية الجنائية والإجرائية، مرجع سابق، ص٦؛

(32) Bouzat . J. pinatel . Traité ole droit penal et de Criminologie . Toml Droit penal , Paris .

(33) *www.fas.org/sgp/crs/homesec/RL30153.pdf*

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

رابعًا – تعريف جريمة اختراق المواقع الإلكترونية الرسمية للدولة بالنظر إلى موضوع الجريمة:

يرى جانب من الفقه بتعريفهم جريمة اختراق المواقع الإلكترونية بالنظر إلى معيار موضوعي، أو بالنظر إلى محل الجريمة، فهم يرون أن الجريمة تكون إلكترونية إذا كان محلها هو الكمبيوتر أو نظامه الكتروني ويعد من أهم المعايير على قدرة إيضاح تعريف الجريمة محل التعريف وذهب الفقيه Rosenblatt بتعريفها على أنها" نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الكمبيوتر أو التي تحول عن طريقه" (٣٥)، كما عرفت بأنها: "كل سلوك غير شمروع او غير مسموح به فيما يتعلق بالمعالجة الاليه للبيانات او نقل هذه البيانات" (٣٦).

ومن جانبه فإن قانون الجرائم المعلوماتية السويسري، قد اشتمل في مواده النص على عقاب من يحصل على البيانات المخزنة إلكترونياً بطريق غير مشروع، وكذلك عقاب من يحصل على البرامج بهدف الحصول على المال على نحو غير مصرح به، أو محاولة الوصول إلى أنظمة الحاسوب وإتلاف محتوياتها أو محو بياناتها(٣٧)

ووجه الانتقاد لهذه التعريفات على انها لا تفرق في وصف الأفعال ولا تحيط بها وإن حاولت الإحاطة بها إلا أنه سيفرق بالتفصيل الذي لا يستقيم وغرض وشكل التعريف كما أنه لا يوجد اتفاق على الأفعال المنطوية تحت وصف جرائم الكمبيوتر(٣٨)، كما أنه ضيق من نطاق الجرائم الإلكترونية التي ترتكب بواسطة الكمبيوتر كالاحتيال الإلكتروني، ولقد سعى الكثير من الدول المتقدمة، إلى تبني ووضع استراتجية قومية بشأن حماية الفضاء الإلكتروني، ففي عام ٢٠٠٠ صدرت مسودة اتفاق عالمي، بشأن جريمة التحريض على الإرهاب عبر وسائل إلكترونية ، وذلك من جامعة" ستاندفورد، والتي سميت بخطة ستاندفورد، وقد تضمنت هذه الخطة العديد من نقاط الإلتقاء، بقصد التوصل إلى تعاون دولي على نطاق واسع، في ما يتعلق بمقاومة هجمات الإرهاب الإلكتروني، وذلك على أساس من القول أن الإرهابيين يقومون باستغلال ثغرات القوانين، وعلى وجه الخصوص مع التطور المتزايد في مجال التكنولوجيا، في مقابل جمود القواعد القانونية في التصدي لأخطار وهجمات الإرهاب الإلكتروني، وقد اقترحت المادة (١٢) من هذه الخطة ضرورة إنشاء وكالة دولية، تهدف إلى تأمين البنية التحتية الكونية للمعلومات(٣٩).

---

(٣٥) هشام محمد فريد رستم، الجرائم المعلوماتية أصول التحقيق الجنائي الفني، مرجع سابق، ص٤٠٧.

(٣٦) هدى قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، ط١، دار النهضه العربية، القاهره، ١٩٩٢م، ص٢٤.

(37) HUET JEROME et MAISL HERBERT, DROIT DE L'INFORMATIQUE ET DES TELECOMMUNICATIONS, DROIT PRIVE ...DROIT PUBLIC, LITEC, 1989, p.868, no. 726.

(٣٧) نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، مرجع سابق، ص٥٧.

(٣٨) نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، مرجع سابق، ص٣٠.

(39) TORTELLO NICOLE & LOINTIER PASCAL, INTERNET POUR LES JURISTES, DALLOZ, 1996, p.2.

وفي هذا الشأن قضت المحكمة الاتحادية العليا بدولة الإمارات العربية المتحدة، بعدم إدانة شخص من تهمة الدخول غير المشروع، متى ثبت عكس ذلك، فقضت بأنه: "ولما كان ذلك وكانت مدونات الحكم المطعون فيه والمؤيد للحكم المستأنف والمكمل له يكشف أن كلا الحكمين قد ألم بظروف الدعوى وملابساتها ومحص أدلة الثبوت فيها وأفصح عن عدم اطمئنانه إليها وحيث ثبت للمحكمة أن المطعون ضده الأول مشترك في خدمة الانترنت بالاتصالات وقدم فاتورة سداد خدمة الانترنت صادرة عن هيئة الاتصالات وأن دخوله لهذه الشبكة مشروع، ولم يثبت لديها أن المتهمين كانا يتجران في المكالمات الدولية ثم انتهى إلى القضاء ببراءتهما مما اسند إليهما، ومن ثم فإن ما تثيره الطاعنة في هذا النعي لا يعدو أن يكون جدل موضوعي حول تقدير المحكمة للأدلة القائمة في الدعوى وهو ما لا يقبل إثارته أمام محكمة النقض"(٤٠).

ويستفاد من هذا الحكم، وفقًا لمفهوم المخالفة، أنه إذا كان الدخول المشروع جائزًا، فإنه من باب أولى يكون الدخول غير المشروع مجرمًا، وبالقياس إذا كان الدخول غير المشروع مجرمًا، فإن الاختراق للمواقع الرسمية أشدًا جرمًا؛ لأنه دخول غير مشروع، ونرى: ضرورة تشديد العقوبة في هذه الحالة؛ لأن جريمته يترتب عليها إضرار بالمجتمع وبالصالح العام.

خامسًا – تعريف جريمة اختراق المواقع الإلكترونية الرسمية للدولة بالنظر إلى الدمج بين عدة تعريفات: رغم محاولات الفقه في سبيل تلافي الانتقادات الموجهه للتعريفات السابقة ذهبوا للدمج بين أكثر من تعريف. وذلك بالنظر إلى معيارين وصف السلوك واتصال السلوك بالمعالجة الآلية للبيانات أو نقلها وتبنت منظمة التعاون الاقتصادي والتنمية عام ١٩٨٣ تعريفًا للجرائم الالكترونية بأنها "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها يعتبر اعتداء على جهاز الكمبيوتر". أو هي "الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات إضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيدًا من الناحية التقنية مثل تعديل الكمبيوتر"(٤١). ويتضح من هذه التعريفات انه يتطلب أن يكون الفعل مما يقع ضمن نطاق قانون العقوبات وهي مسألة جدل لهذه التعريفات حول مدى انطباق قواعد التجريم التقليدية على هذه الأفعال مما يؤدي إلى ضرورة الحاجة لنصوص خاصة تفرد أحكامها بقانون الجرائم الإلكترونية مراعية العناصر والسمات الطبيعية لهذه الجرائموالحقيقة أنه تعددت التعريفات للجريمة الإلكترونية وتباينت وجاءت قاصرة عن الإحاطة بأوجه ظاهرة الإجرام الإلكتروني التي تتلائم مع طبيعة هذه الظاهره التي تختلف عن غيرها من الجرائم التقليدية وازاء ذلك فنجد باستقراء التعريفات السابقة التي تضمنت

---

(٤٠) دولة الإمارات العربية المتحدة: المحكمة الإتحادية العليا – الأحكام الجزائية – الطعن رقم ١٨٥ لسنة ٢٠١١ قضائية بتاريخ: ٢٠١١/٦/٢١م.

(٤١) محمود مدين، الجريمة الإلكترونية وتحديات الأمن القومي، المصرية للنشر والتوزيع، القاهرة، ٢٠١٩م، ص٢٨.

التعريف للجرائم االلكترونية بأن النماذج المعروضه للتعريف ركزت على وسيلة ارتكابها والى الغاية والى شخصية الفاعل وركز جانب اخر إلى دمج هذه التعريفات بتعريف واحد ولمحاولة تعريف الجرائم االلكترونية وتفادي اوجه القصور التي شابت هذه التعريفات فقد تبنى حديثًا مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا في شهر أبريل عام ٢٠٠٠ تعريفًا جامعًا لجرائم الكمبيوتر اقرب للشمولية وعرف الجريمة الإلكترونية على انها "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام كمبيوتر وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"[١]. ونجد ان هذا التعريف قد أحاط أحاط بجميع صور الجريمة الإلكترونية التي تقع بواسطة نظام إلكتروني أم داخل النظام من معطيات وبرامج ومعلومات وشموله أيضًا جميع الجرائم الواقعة في بيئة إلكترونية وهو بذلك يعد من افضل التعريفات التي تناولت ظاهره الاجرام االلكتروني ، ومن ثم فأنه يمكن تعريف الجرائم الإلكترونية على أنها عمل غير مشروع مخالف للقانون من شخص مسؤول بالاعتداء على البيانات أو المعلومات المخزنة على جهاز الكمبيوتر او على وسيلة تقنية اخرى سواء كان هذا العمل باستخدام جهاز الكمبيوتر او شبكة الانتر نت او وسلية تقنية اخرى يقرر لها القانون عقوبة جنائية او تدبيراً احترازيًا من أجل إلحاق الضرر بالآخرين"، وفضلا عن ذلك فاذا تعددت التعريفات للجريمة الإلكترونية من جانب الفقه وتباينت فيما بينهما ولم يتسنى وجود مصطلح قانوني موحد للدلالة على تعريفها فأن الأمر لا يختلف عنه في التشريعات الجنائية التي لم تضع معظمها تعريفًا للجريمة االلكترونية فهذا ليس بقصور لأن وضع التعريف ليس من عمل المشرع وإنما هو من اختصاص الفقهاء[٢]، وذلك أن الأمر لا لا يحول دون الاجتهاد في تفسير النصوص العقابية التقليدية التي تعاقب على صور الاعتداء المختلفة بحيث يمكن تطبيقها على الجرائم المبتكره مما يجد المشرع نفسه مضطراً إلى ذلك أما لتحديد الأركان العامة والخاصة للجريمة أو لأن السلوك الجنائي من الصور المبتكره[٣]، فنجد ان المشرع المصري[٤] المصري[٤] لم يتناول تعريف الجريمة االلكترونية وحاله بذلك كحال التشريعات الجنائية الأخرى، إلا انه

---

(١) محمد أمين الشوابكة، جرائم الحاسوب والإنترنت الجريمة المعلوماتية، مرجع سابق، ص١٠.

(٢) عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، مرجع سابق، ص١٨.

(٣) بهاء المري، شرح قانون مكافحة جرائم تقنية المعلومات وحجية الدليل الرقمي في الإثبات، العربية للنشر والتوزيع، القاهره، ٢٠١٩م، ص١٥.

(٤) ومما تجدر الإشارة إليه في هذا الصدد، أن المشرع المصري قد تنأول في عدد من التشريعات الخاصة، ذات الصلة بوسائل الجريمة المعلوماتية، ومن هذه التشريعات، قانون مصلحة الأحوال المدنية رقم (١٤٣) لسنة ١٩٩٤م وكذلك قانون غسيل الأموال رقم (٨٠) لسنة ٢٠٠٢م، وقانون الملكية الفكرية بشأن رقم (٨٢) لسنة ٢٠٠٢م، وقانون تنظيم الاتصالات رقم (١٠) لسنة ٢٠٠٣م، وقانون التوقيع الإلكتروني رقم (٣٥) لسنة ٢٠٠٥م، وقد الفقرة (أ) من المادة الأولى من القانون الأخير الكتابة الإلكترونية بأنها: "كل حروف أو أرقام أو رموز أو أية علامات أخرى تثبت على دعامة إلكترونية أو ورقية أو ضوئية أو أي وسيلة أخرى مشابهة وتعطي دلالة قابلة للإدراك".

انه تناول صوراً لتلك الجرائم في القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات في ثلاثة فصول تناول في الأول منها جريمة الاعتداء علي سلامة شبكات وأنظمة وتقنيات المعلومات وصورها (جريمة الانتفاع بدون حق بخدمات الاتصالات والمعلومات وتقنيتها)، وجريمة الدخول غير المشروع، وجريمة تجاوز حدود الحق في الدخول، وجريمة الاعتراض غير المشروع، وجريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية، جريمة الاعتداء على البريد الإلكتروني أو الموقع أو الحسابات الخاصة، وجريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة، جريمة الاعتداء علي سلامة الشبكة المعلوماتية. وفي الفصل الثاني تناول الجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات وصورها جرائم الاحتيال والاعتداء علي بطاقات البنوك والخدمات وأدوات الدفع الإلكتروني، والجرائم المتعلقة باصطناع المواقع والحسابات الخاصة بالبريد الإلكتروني. وفي الفصل الثالث تناول الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتي غير المشروع. فلا يجوز المساس بمحتوي البريد الإلكتروني أو تفتيش هذا المحتوي داخل الكمبيوتر أو الإطلاع علي مكنونه أو أسراره بالتنصت أو التفتيش إلا بإذن قضائي مسبب ، وهو ما اضطرد عليه القضاء الأمريكي في العديد من الأحكام(١)

وفي هذا الخصوص قررت محكمة تمييز دبي أنه: "إذا ورد في النص التشريعي لفظ مطلق ولم يقم الدليل على تقييده فقد أفاد ثبوت الحكم على إطلاقه ولما كانت المادة ٤٦ من القانون رقم ١/٩١ تنص على عقاب كل من يستخدم الأجهزة أو الخدمات أو التسهيلات التي تقدمها المؤسسة في الإزعاج أو إيذاء مشاعر الآخرين أو أي غرض آخر غير مشروع وكانت هذه العبارة الأخيرة قد وردت على سبيل الإطلاق في مجال بيان الأعمال المؤثمة مما مفاده شمول الحظر لكل فعل غير مشروع في نطاق إعمالها أيا كانت طبيعته طالما خرج عن الغرض المحدد له في استخدام الشبكة طبقًا للشروط المنصوص عليها في المادة ١٢ من القانون والمعاقب عليها بالمادة ٤٥ منه، لما كان ذلك وكان الحكم المطعون فيه وفى حدود السلطة التقديرية في التفسير والتكييف قد أورد في أسبابه أن الغرض غير المشروع على إطلاق عبارة النص يشمل كل فعل أو امتناع عن فعل تجرمه القوانين أو اللوائح وأن ما قام به المتهم باعترافه من اختراقه لشبكة الاتصالات الانترنت التابعة لمؤسسة الإمارات مستخدماً برامج للبحث عن الثغرات واستطاع بذلك الحصول على كلمات السر لبعض المواقع المحظورة على غير موظفي المؤسسة الدخول إليها وقام بفك شفرة بعض الأجهزة ونسخ بعض الملفات وهو يعلم بحظر ذلك لغير موظفي المؤسسة المرخص لهم بذلك كما قام بفك رسائل البريد الالكتروني لبعض الموظفين

(1) Kataz, Berger . v . New York , 388 , U . S . , 41 1967. . www.lex.electronica–org/articles,v6–21pepin.htm.

ونقلها إلى جهاز الحاسب الآلي الخاص به مما يشكل استغلالًا للشبكة لغرض غير مشروع يوقعه تحت طائلة العقاب وهي أسباب سائغة تتفق وصحيح القانون وتتوافر بها كافة الأركان القانونية للتهمة الأولى المسندة إلى الطاعن مما يكون معه منعه في هذا الخصوص غير سديد لما كان ذلك وكانت خدمة الانترنت تدخل ضمن الخدمات التي تقدمها مؤسسة الاتصالات وتخضع لأحكام القانون رقم ١/٩١ الخاص بمؤسسة الاتصالات فإن ذلك لا يتعارض مع عدم صدور تشريع خاص بخدمات الانترنت ويكون منعي الطاعن في هذا الصدد غير مقبول"[١].

المطلب الثاني

خصائص جريمة اختراق المواقع الإلكترونية الرسمية للدولة

انفردت الجرائم الإلكترونية بخصائص وميزات ميزتها عن الجرائم التقليدية نظراً لطبيعتها التي ترتكب في بيئة غير تقليدية تقع خارج إطار الواقع المادي الملموس يطلق عليها البيئة الإلكترونية من حيث أنها تكتسب خصوصية غير عادية وهي جرائم جديدة في شكلها ووسائلها ومخاطرها بلون وثوب جديدين وهذه الخصائص سنتناول اهمها، وذلك على النحو الآتي:

أولًا – جريمة اختراق المواقع الإلكترونية الرسمية للدولة جريمة عالمية عابرة للحدود: أطلق على شبكة الإنترنت الإمبراطورية التي لا تغيب عنها الشمس[٢]، فبعد ظهور هذه التقنية أذيبت جميع الحدود الجغرافية الفاصلة بين دول العالم ولم تعد تخضع لنطاق إقليمي محدود ولم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات فأسفر نقل وتبادل المعلومات بين أنظمة الكمبيوتر لأماكن متباعدة إلى نتيجة مؤداها أن أماكن متعددة في دول العالم المختلفة قد تتأثر بالجريمة الإلكترونية الواحدة في نفس الوقت فالجريمة الإلكترونية لا تعترف بحدود وهي شكل جديد من أشكال الجرائم العابرة للحدود الإقليمية بين الدول كافة[٣]، واضف لذلك فالجريمة الإلكترونية تعبر الزمان والمكان دون الخضوع لحرس حدود ونقاط تفتيش. فمفهوم الجريمة الإلكترونية أصبح عالمياً وترتكب في أكثر من دولة، فالفاعل ليس موجوداً بل يرتكب جريمته عن بعد مما يعني عدم تواجده المادي في مكان ومسرح الجريمة فتتباعد المسافات بين الفعل الذي يتم من خلال جهاز الكمبيوتر للفاعل وبين محل الاعتداء فهي ترتكب بدون حركة تنقل ما بين الدول فيوجد الفاعل في بلد ما ويستطيع الولوج إلى جهاز كمبيوتر

---

(١) حكومة دبي: محكمة التمييز – الأحكام الجزائية – الطعن رقم ٢٣٠ لسنة ٢٠٠١ قضائية – الدائرة الجزائية – بتاريخ: ٨-١٢-٢٠٠١م – مكتب فني ١٢ رقم الجزء ١ رقم الصفحة ١٢٦٦.

(٢) محمد عبد الرحيم سلطان، جرائم الإنترنت والاحتساب عليها، مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات، العين، مايو ٢٠٠٠م، ص٢٢.

(٣) خالد ممدوح إبراهيم، الجريمة المعلوماتية، ط٢، دار الفكر الجامعي، الإسكندرية، ٢٠١٩م، ص٨٨.

لأحد الأشخاص أو المؤسسات في بلد آخر وهو ما قد يلحق الضرر بآخرين في بلد ثالث[١] وهي بذلك تخضع لأكثر من قانون جنائي فتعتبر شكلًا جديداً من الجرائم العابرة للحدود الوطنية او الاقليمية.

فلا حدود جغرافية ولا فواصل حديدية في شبكة الإنترنت؛ حيث زالت الحدود والعوائق بين الدول وبعضها، بموجب الإنترنت وأحكامه؛ فيسهل التواصل بين أشخاص بينهم آلاف الأميال، فى ذات الوقت على شبكة الإنترنت، وعلى ذلك فإن الجرائم التي ترتكب عبر الإنترنت، تتم عبر الدردشة؛ بحيث تتجاوز حدود الدول التى ارتكبت فيها، لتتعدى آثارها جميع دول العالم.

ثانيًا – سهولة ارتكاب جريمة اختراق المواقع الإلكترونية الرسمية للدولة: تمتاز الجريمة الإلكترونية بصورة واضحة في أسلوب ارتكابها فالجرائم التقليدية يتطلب ارتكابها مجهوداً عضلي كالعنف والإيذاء بعكس الجريمه الإلكترونية التي يتطلب ارتكابها أسلوب هادئ فهي لا تحتاج لعنف لذا تعد جرائم ناعمه واطلق عليها بعض الفقه مصطلح جرائم ذوي الياقات البيضاء[٢]، فتنوعت الأساليب المستخدمة في ارتكابها فالمجرم الإلكتروني يستطيع تنفيذ مخططه الإجرامي لوحده وأمام الكمبيوتر وهو جالس بمنزله أو مكتبه أو في مقهى للإنترنت فكل ما يحتاجه سوى عدد من اللمسات على أزرار لوحة المفاتيح حتى تؤدي إلى إسقاط الحواجز الأمنية للنظم والشبكات[٣]، أو إتلافها وتحريفها وتزويرها وسرقتها أو باستخدامها كوسيلة لارتكابها جريمة إلكترونية أخرى[٤]. فهي من الجرائم النظيفة فلا اثار فيها لاية عنف او دماء وانما اثاراها ارقام وبيانات فارتكابها لا يستغرق الثواني وليس شأنها شأن بقية الجرائم التقليدية ذات الأثر المادي.

ثالثًا – جريمة اختراق المواقع الإلكترونية الرسمية للدولة ترتكب بعيداً عن الأنظار: تتصف الجرائم الإلكترونية بأنها مستترة فالمجني عليه لا يلحظها مع أنها تقع أثناء وجوده على الشبكة فالجاني يرتكبها بخفة شديدة ودون أن يرى أطرافها (سواء الجاني أو الضحية)، فيقوم الجاني بالتعامل مع نبضات إلكترونية غير مرئية لا يمكن قرائتها إلا بواسطة الكمبيوتر[٥]، كما ان الضحية لا يشاهد مرتكب الجريمة (الجاني) فقد تعد مربحة للجاني وفي ذات الوقت مكلفة على الضحية مما يتسبب بإلحاق أضرار مالية بليغة بحقه مقارنة بما يمكن أن تتسبب به الجريمة التقليدية فهي جرائم فنية تقنية في الغالب الأعم والجاني يكون من ذوي الاختصاص في مجال التقنية والتعامل مع شبكات الكمبيوتر او

---

(١) محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، مرجع سابق، ص٣٧.

(٢) أسامة أحمد المناعسة، وجلال محمد الزعبي، جرائم تقنية نظم المعلومات الالكترونية – دراسة مقارنة، ط٣، دار الثقافة للنشر وتوزيع، عمان – الأردن، ٢٠١٧م، ص٩٧.

(٣) نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، مرجع سابق، ص٥٢.

(٤) محمد حماد مرهج الهيتي، جرائم الحاسوب – دراسه تحليلية، ط١، دار المناهج، عمان – الأردن، ٢٠٠٦م، ص٢١٢.

(٥) هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص٤٢.

بيانات مجمعة ومجهزة للدخول للنظام الالكتروني بغرض معالجتها إلكترونياً بما يُمكن المستخدم من إمكانية كتابتها من خلال العمليات المتبعة وهذه العمليات وثيقة الصلة بارتكاب الجرائم ولابد من ذكاء وفهم الجاني على ارتكابها(١).

رابعًا – جريمة اختراق المواقع الإلكترونية الرسمية للدولة من الجرائم المستمرة: صعب اختراق الأجهزة الأمنية للتنظيمات الإرهابية الإلكترونية، التي تسلك أسلوب الجرائم المعلوماتية؛ وذلك نظراً لطبيعة هذه الجريمة، وتفرق أفرادها في أماكن جغرافية متباعدة، هذا بالإضافة إلى أن الإرهاب الإلكتروني لا يخلف خلفه أية آثار مادية؛ بحيث لا يمكن تتبعه بسهولة للوصول إلى الجاني، فهو مجرد أرقام تتغير في السجلات الرقمية بصفة دائمة ومستمرة، وهذه الصعوبات تؤدي إلى ضعف قوى الرصد والمتابعة لدى الأجهزة الأمنية، وهو ما يؤدي بدوره إلى استمرارية التنظيم الإرهابي الإلكتروني، مع المزيد من المناورات والتحركات(٢).

ومن هذه الصور ما قضت به المحكمة الاتحادية العليا(٣)؛ حيث قضت بمعاقبة إرهابيين إلكترونيين؛ وطلبت معاقبتهما بما ورد في القانون الاتحادي رقم (٧) لسنة ٢٠١٤م في شأن مكافحة الجرائم الارهابية؛ حيث نسبت إليهما المحكمة تهمة ارتكاب جريمة إرهابية إلكترونية، وذلك بانضمامهما إلى تنظيمات وجماعات وميليشيات إرهابية، والترويج لأفكارها عبر الإنترنت(٤)، وكذلك ما ما قضت به ذات المحكمة، بسريان أحكام هذا القانون في شأن جريمة السب والقذف باستخدام الشبكة المعلوماتية(٥).

ونلاحظ: في هذا الحكم أن المشرع الإماراتي لم يهمل القانون الاتحادي رقم (٢) لسنة ٢٠٠٦م في شأن مكافحة الجرائم الإرهابية؛ في تطبيق أحكامه على الجرائم الإرهابية ذات الطابع الإلكتروني، **وهو ما نراه – في اعتقادنا** – كدلالة على يقظة القضاء الاتحادي، وعدم تقيده بقانون واحد، وإنما استخدم من القوانين ما يناسب كل جريمة من عقوبات.

---

(١) أحمد خليفة الملط، الجرائم المعلوماتية، ط٢، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م، ص١٠٥.

(٢) عبد المجيد الحلاوي، أهمية التعاون العربي والدولي في محكافحة جرائم الإرهاب المعلوماتي، بحث ضمن دورة تدريبية بعنوان: مكافحة الجرائم الإرهابية المعلوماتية، خلال الفترة من: ١١-١٤٢٧/٣/١٥هـ، الموافق ٩- ٢٠٠٦/٤/١٣م، المغرب – القنيطرة، ص٩ وما بعدها. متاح على شبكة المعلومات الدولية عبر الرابط الإلكتروني:

http://repository.nauss.edu.sa/bitstream/handle

(٣) المحكمة الإتحادية العليا، دائرة الأحكام الجزائية، الطعن رقم ١، لسنة ٢٠١٥ قضائية، بتاريخ ٢٠١٥/٦/١٦م.

(٤) الحكم متاح على شبكة قوانين الشرق عبر الرابط الإلكتروني:http://site.eastlaws.com.

(٥) المحكمة الاتحادية العليا، دائرة الأحكام الجزائية، الطعن رقم ٤٨٣، لسنة ٢٠١٦ قضائية، بتاريخ ٢٠١٦/١٢/٩م.

خامساً – جريمة اختراق المواقع الإلكترونية الرسمية للدولة يصعب اكتشافها واثباتها: تقع الجريمة الإلكترونية في بيئة افتراضية تقنية لا تترك ولا تخلف أية آثار ملموسة إذ يغلب طابع السرية عليها فالجناة يعمدون في كثير من الأحيان إلى إخفاء نشاطهم الجرمي عن طريق التلاعب بالبيانات التي تتحقق بغفلة عن المجني عليه مما يصعب معه الحصول على دليل مادي لمثل هذه الجرائم التي يحيط بها كثير من الصعوبات المتمثلة في صعوبة اكتشافها فهي لا تترك أثراً خارجياً حيث يغلب عليها الطابع التقني(١). ومغزى الأمر في هذه الجرائم انها لا تترك أية آثار خارجية فلا يوجد جثث أو قتلى أو آثار دمار أو كسر كما هو الحال في الجرائم التقليدية فيمكن ان يكون اكتشافها بالصدفة(٢).

ونحن نرى: أن المشرع الإماراتي قد تصدى لجريمة اختراق المواقع الرسمية للدولة، ليس على المستوى الأمني فحسب، بل على المستوى الثقافي والاجتماعي، وذلك من خلال العديد من الإصدارات والدوريات، التي تهدف إلى توعية المجتمع بخطر الاختراق الإلكتروني، ولا ينسى الدور المهم الذي تلعبه أكاديمية شرطة دبي(٣) في التصدي لخطر اختراق المواقع الرسمية للدولة.

ومما يزيد من صعوبة اكتشافها ذلك أن كثير من هذه الجرائم لا يتم الإبلاغ عنها من المجني عليه خاصة شركات ومؤسسات الأعمال إما لعدم اكتشاف الضحية أو خشية من التشهير(٤)، فيصعب معرفة مرتكبها فهي كما اشرنا سابقًا انها ترتكب في بيئة افتراضية فلا يترك مرتكبها اثاراً مما يزيد الامر صعوبة على المحقق الجنائي التقليدي في فهم حدودها وما تخلفه من اثارها غير المرئية ذلك ان الدليل الاكتروني بها هو يعد وسيلة الاثبات لامكانية تعقب اثر مرتكبها فهذه الوسيلة من السهوله طمسها واخفائها او تدميرها في لا تقدر الزمان والمكان فملاحقة مرتكبها يكون بحاجة إلى تعاون دولي حقيقي(٥) وسنأجل الحديث عن هذه الصعوبات والمعوقات عند الحديث عن معوقات التحقيق الجنائي في الباب الثالث من هذه الدراسة.

---

(١) نبيل عبد المنعم جاد، أسس التحقيق والبحث الجنائي العلمي، مطبعة كلية الشرطة، القاهرة، ٢٠٠٥م، ص٣٧٣.

(٢) نائل عبد الرحمن صالح، واقع جرائم الحاسوب في التشريع الأردني، مرجع سابق، ص٣.

(٣) التعريف بالأكاديمية: "أنشئت كلية شرطة دبي عام ١٩٨٧م بمقتضى القانون رقم (١) لسنة ١٩٨٧م، وبدأت الدراسة رسمياً في التاسع عشر من سبتمبر لعام ١٩٨٧م، انطلاقًا من مدرسة تدريب الشرطة بإدارة الطوارئ في حينه، إلى أن اكتمل مبنى الأكاديمية في شكله الحالي، واكتملت البنية الأساسية للكلية في شهر أكتوبر من عام ١٩٨٨م بعد إصدار القرار رقم (١) لسنة ١٩٨٨ في شأن اللائحة الداخلية لكلية الشرطة، وافتتحـــــت الكلية رسميـــــًا في الأول من أبريل عام ١٩٨٩م ".

https://www.dubaipolice.ac.ae.

(٤) محمود عبد العزيز أبو زيد، الحماية الجنائية لتكنولوجيا الحاسب الآلي والنظم المعلوماتية، رسالة دكتوراه، كلية الحقوق – جامعة القاهرة، ٢٠١٦م، ص١٦٦.

(٥) عبد الاله النوايسة، جرائم تكنولوجيا المعلومات – شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، ط١، دار وائل للنشر والتوزيع، عمان – الأردن، ٢٠١٧م، ص٨٠.

سادسًا – جريمة اختراق المواقع الإلكترونية الرسمية للدولة تعتمد على استخدام التقنية الرقمية لارتكاب الجريمة: لقد دأبت التنظيمات الإرهابية المعاصرة على مواكبة التطورات العلمية والتكنولوجية، واستخدام وسائل الاتصالات الحديثة؛ حيث يعتمد الإرهاب الإلكتروني على هذه الوسائل الإلكترونية لاختراق النظم المعلوماتية الحساسة في الدولة وتخريبها، وبمعنى أدق فهو يستعملها كحلقة وصل لربط أجهزته الرقمية مع الشبكات المعلوماتية الحساسة؛ بغية استهدافها فيما بعد، فيلجأ الإرهابيون، إلى استعمال التقنيات الرقمية، من خلال الحاسب الآلي المتصل بشبكة الإنترنت؛ وذلك بقصد بث الإشاعات والفوضى، وتخويف وترويع أفراد المجتمع، سواء كانوا أشخاصا طبيعيين؛ كالأفراد، أو معنويين، كالدولة ومؤسساتها، أو لمهاجمة نظم المعلومات، بتدمير المواقع وبث الفيروسات، وهو ما كان ملجأ آمنًا لكثير من المنظمات الإرهابية في إنشاء العديد من المواقع؛ بقصد نشر أفكارهم ومعتقداتهم، والتخطيط والتجهيز للعمليات الإرهابية، وتنسيق وتبادل الخبرات العملية؛ حيث تم اكتشاف العديد من المواقع التابعة للإرهابيين، والتي تهدف إلى تعليم صناعة الألغام والمتفجرات والعبوات الناسفة، والأسلحة الكيماوية الفتاكة، فضلًا عن وسائل تسميم المياه، والتخطيط لتفجير الميادين العامة والأسواق، وتدمير المواقع والبيانات والنظم الرقمية والبريد الإلكتروني، وطرق الوصول إلى المواقع المحجوبة، وبث الفيروسات المدمرة للأجهزة[١].

وفضلًا عن ذلك، المواقع المخصصة للحرب النفسية على المجتمع والدول؛ وذلك من خلال عرض العصابات الإرهابية للأسرى والرهائن، وكيفية إعدامهم وتعذيبهم[٢].

وهوما يمكن معه القول، بأن أمن المجتمعات الآن، ليس مهدداً بالطائرات والصواريخ والقنابل الذرية، بقدر ما هو مهدد كذلك بأجهزة الكمبيوتر والإنترنت؛ وذلك من خلال البرامج المتطورة التي من شأنها أن تؤدي إلى تدمير البنية الأساسية للدولة المستهدفة، وتخريب معداتها الدفاعية ووسائل اتصالاتها وأنظمتها العسكرية وقوى الطاقة بها[٣].

سابعًا – جريمة اختراق المواقع الإلكترونية الرسمية للدولة من الجرائم الخطرة: هذه الخاصية من أهم خصائص الإرهاب الإلكتروني، وهي خاصية ليست مستقلة بذاتها، بل مكملة للخاصية التي سبقتها؛ حيث إن استعمال التقنيات الحديثة، هي التي بها قوام الحياة، بحيث لا يمكن بحال الاستغناء عنها، فإن استخدامها بأساليب سيئة أو ضارة، أدت إلى ظهور نوع من الإجرام المستحدث الذي يهدد العالم

---

(١) من هذه المواقع على سبيل المثال: موقع سرايا الجبل، وموقع قناص، وموقع مشاور، وغيرها.

(٢) نبيلة هبة هروال، جرائم الإنترنت – دراسة مقارنة، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد – الجزائر، ٢٠١٣م/ ٢٠١٤م، ص٣٣٦.

(٣) عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، مرجع سابق، ص١٨٩.

بأكمله، وهو الإرهاب الإلكتروني، وعلى وجه الخصوص في الدول التي تعتمد بصورة كبيرة على تكنولوجيا المعلومات؛ وهي تكون هدف الإرهابيين الأول والأنسب، فإن الإرهاب الإلكتروني من الممكن أن يؤدي إلى إلحاق الضرر بالدولة المتقدمة؛ ومن ثم حدوث شلل تام بأنظمة القيادة لديها والسيطرة والاتصالات، وذلك عن طريق قطع شبكة الاتصالات بين القيادة ووحداتها، أو تعطيل وإفشاد أنظمة الدفاع الجوية، أو عن طريق إخراج الصواريخ المطلقة عن مسارها المحدد لها، وكذلك من الممكن اختراق البنوك والمؤسسات المالية، وإحداث حالة من الارتباك في خطوط الطيران، كتعطيل محطات الطاقة الحرارية أو النووية.

وعلى ذلك يتميز الإرهاب الإلكتروني بأنه من أخطر الجرائم التي يواجهها العالم المعاصر؛ حيث صار بإمكان الإرهابي بمجردة الضغط على أزرار لوحة المفاتيح الخاصة بجهازه، أن يختزل أكثر من تسعين بالمائة من أعماله الإرهابية، كما يمكنه الحصول على أسلحة أو متفجرات أو قنابل وهو في بيته، وذلك من خلال المواقع المخصصة لهذا الغرض، فهو يعتمد على البرمجيات كسلاح، وما أسهل الحصول على هذه البرمجيات بواسطة الإنترنت، كما من الممكن توزيع هذه البرمجيات بصورة عشوائية، ومن ثم تحميلها على مواقع مجهولة والقيام بالدعوة إليها، وهو ما يدفع الكثير إلى الدخول إلى هذه المواقع لمعرفة محتواها ومضمونها، وكثير من الزائرين يتأثر بهذه المواقع وينضم إلى كتيبة الإرهاب، فيزداد تبعًا لذلك عدد أفراد الجماعات الإرهابية[١].

ثامنًا – مرتكب جريمة اختراق المواقع الإلكترونية الرسمية للدولة في الغالب شخص خبير في مجال الإلكترونيات: مرتكب جريمة مخترق هو شخص على دراية تامة، ولديه خبرة كبيرة واطلاع واسع في مجالات استخدام الكمبيوتر؛ لارتكاب جريمته الإلكترونية عبر شبكة الإنترنت، وعلى ذلك فإن غالبية من يرتكبون جرائم الإرهاب الإلكتروني هم من المهندسين والخبراء؛ مما يجعلهم يمتلكون قدرات خارقة في التحكم والسيطرة على برامج الكمبيوتر، بقصد تحقيق أهدافهم[٢].

تاسعًا – جريمة اختراق المواقع الإلكترونية المواقع الإلكترونية الرسمية للدولة يستهدف النظم المعلوماتية: تكمن الأهداف الأساسية لجرائم الإرهاب الإلكتروني في الحصول على المعلومات والبيانات الإلكترونية، المحفوظة على أجهزة أجهزة الكمبيوتر، أو المنقولة عبر شبكة المعلومات

---

(١) عبد الحميد إبراهيم محمد العريان، العلاقة بين الإرهاب المعلوماتي والجرائم المنظمة: ما هو رد فعل القطاع الخاص، بحث ضمن دورة تدريبية بعنوان: مكافحة الجرائم الإرهابية المعلوماتية، خلال الفترة من: ١١-١٤٢٧/٣/١٥هـ، الموافق ٩- ٢٠٠٦/٤/١٣م، المغرب – القنيطرة. ص١٢.

(٢) المرجع السابق، الموضع نفسه.

الدولية؛ حيث تساعدها هذه المعلومات في كيفية الوصول إلى أهدافها الإرهابية[١]، والتي تصدى لها المشرع الإماراتي والقانون رقم (٢) لسنة ٢٠٠٦م بشأن مكافحة جرائم تقنية المعلومات[٢]، وتعديله رقم (٥) لسنة ٢٠١٢م[٣].

وعليه فإن المعلومات ليست مقصودة بذاتها، وإنما يراد منها الوصول إلى تحقيق أهداف أخرى؛ كالاستيلاء على أموال البنوك لتدبير نفقات العمليات الإرهابية، كما يمكن من خلال هذه المعلومات الوصول إلى الأشخاص أو الجهات المستهدفة.

ويتبين من ذلك، أن من أهم ما يميز الإرهاب الإلكتروني، أنه يستهدف دائمًا النظم المعلوماتية؛ باعتبارها الحد الفاصل بينه وبين صور الإرهاب الأخرى؛ حيث تعتبر هذه المعلومات والبيانات هدف الإرهاب المباشر لتنفيذ مخططاته التخريبية، وهي أيضًا وسيلة آمنة لتحقيق أهدافه غير المباشرة، والتي تكمن في إيجاد حالة من الرعب والخوف داخل المجتمع، ومن ثم التأثير على الرأي العام، فضلًا عن ما يؤدي إليه من خسائر فادحة في الاقتصاد القومي للبلاد، نتيجة لتعطيل سير المرافق الاقتصادية والاجتماعية العامة والخاصة[٤].

المطلب الثالث

صور جريمة اختراق المواقع الإلكترونية الرسمية للدولة

بعد استعراض تعريف الجريمة الالكترونية واهم الخصائص المميزه لها سنقوم بتقسم هذه الجرائم على هدي التقسيم الشائع في الدراسات والابحاث الامريكية للجرائم المرتكبه عبر الشبكة الدولية وخاصة مشروع القانون النموذجي لجرائم الكمبيوتر والانترنت الموضوعه سنة ١٩٩٨، الذي قسم هذه الجرائم إلى جرائم الاعتداء على الأشخاص وجرائم الاعتداء على الأموال[٥] فالصور الاكثر شيوعًا لجرائم الكمبيوتر هي اولًا جرائم الأموال وثانيًا جرائم الأشخاص وسوف نتناولها في هذا المطلب الجرائم الواقعه على الأموال، والجرائم الواقعه على الأشخاص، وذلك على النحو الآتي:

أولًا – جريمة اختراق المواقع الإلكترونية الرسمية للدولة الواقعه على الأموال: أسفر الواقع المعاصر عن ان الجرائم المرتكبة على الأموال والاتصالات من اخطر الجرائم الالكترونية المستحدثه

---

(١) عبد الله علي عبد الله القحطاني، إدارة أمن المعلومات ودورها في الحد من الإرهاب الإلكتروني بكلية الحسابات وتقنية المعلومات بجامعة الملك عبد العزيز بجدة، رسالة ماجستير، جامعة نايف للعلوم الأمنية، الرياض – المملكة العربية السعودية، ١٤٣٨هـ/٢٠١٧م، ص٣٦.

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

(٣) الجريدة الرسمية العدد ٥٤٠ ملحق السنة الثانية والأربعون – بتاريخ ٢٠١٢/٨/٢٦م.

(٤)عبد المجيد الحلاوي، أهمية التعاون العربي والدولي في محكافحة جرائم الإرهاب المعلوماتي، مرجع سابق.

(٥) يونس عرب، جرائم الانترنت، إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الاجرائية للملاحقة والإثبات، ورقة عمل، مقدمه إلى مؤتمر الأمن العربي، ٢٠٠٢م، المنظم بالمركز العربي للدراسات والبحوث الجنائية، أبوظبي، في ٢٠١٢/١٢/١٠م.

كون هذه الجرائم تؤدي للكثير من الخسائر المادية الضخمه فالجرائم التقليدية لا تتم إلا بالسطو على المؤسسات المالية او الشركات وهي بذلك تحتاج إلى تخطيط مسبق ومجهود عضلي جماعي بخلاف الجرائم المالية اللكترونية التي تتم بسهوله فكل ما تحتاجه ان يتوافر لدى الجاني الدراية الكافية ببرامج الكمبيوتر كما انها لا تحتاج لمجهود جماعي بل يكفي ان يرتكبها شخص او اثنان لارتكابها ومن الجرائم الواقعه على الأموال كجرائم الاحتيال والاعتداء على بطاقات البنوك [١] والخدمات وادوات الدفع اللكترونية[٢] حيث انه يتطلب في هذه الجريمة الاخيرة توافر الركن المادي المتمثل بقيام الجاني بقراءة بيانات البطاقات البنكية باستخدام رقاقات الراديو اللاسلكية ودون حاجة للمس حامل البطاقه بحيث يتمكن الجاني من تصفح واستخدام حساب المستخدم في مواقع مختلفه وكذلك لا بد من قيام الركن المعنوي المتثل في ان يكون الجاني على علم وارادة بحقيقة سلوكه الاجرامي كما يلزم توافر قصداً خاص بان ما يحصل عليه الجاني من معلومات اوبيانات للبطاقات البنكية هو بغرض الحصول على أموال الغير،وبالاضافة لهذه الجرائم فانه يعد من اخطر الجرائم المالية غسيل الأموال التي تتم باساليب وشكال متعدده تتدرج من البساطه إلى التعقيد وقد كان للتكنولوجيا دور كبير في تطوير الاساليب التي تستخدم لغسيل الأموال ولعل التهريب هو ابسط واقدم الطرق التي يستخدمها الأشخاص محترفي عمليات غسيل الأموال، كما استخدمت اساليب اخرى مثل شركات الواجهه والقيام ببعض التصرفات العينية المادية[٣]

ثانيًا – جريمة اختراق المواقع اإلكترونية الرسمية للدولة الواقعه على الأشخاص: جميع جرائم الكمبيوتر ليست فقط جرائم أموال، بل يمكن تصورها ايضاً كجرائم أشخاص ترتكب باستخدام جهاز الكمبيوتر او اجهزة الاتصالات ويكون محلها الأشخاص ومن ذلك على سبيل المثال جرائم القذف والسب والاعتداء على الحياة الخاصة[٤] والاخلال بالاداب العامه[١] بالاضافة إلى جريمة التهديد

---

(١) هدى قشقوش، جرائم الحاسب اإلكتروني في التشريع المقارن، مرجع سابق، ص١١٤ وما بعدها؛ محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مرجع سابق، ص١٠٥.

(٢) ومنه ما نصت عليه المادة (٢٣) من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات المصري على أن: "يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامه لا تقل عن ثلاثين ألف جنية، ولا تجاوز خمسين ألف جنية أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أو بطاقات البنوك والخدمات أو غيرها من أدوات الدفع اإلكتروني".

(٣) محمد إبراهيم محمد الشافعي، النقود اإلكترونية، مجلة الأمن والحياة، أكادمية شرطة دبي، يناير٢٠٠٤م، ص١٢ وما بعدها.

(٤) نصت المادة (٣٥) من القانون الإماراتي رقم (٥) لسنة ٢٠١٢م بشأن مكافحة جرائم تقنية المعلومات على أنه: "مع عدم الإخلال بالأحكام المقررة في الشريعة الإسامية، يعاقب بالحبس والغرامة التي لا تقل عن مائتين وخمسن ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتن العقوبتن كل من ارتكب عن طريق الشبكة المعلوماتية أو وسيلة تقنية معلومات أو على موقع إلكتروني، إحدى الجرائم التالية:

١- الإساءة إلى أحد المقدسات أو الشعائر الإسلامية.

٢- الإساءة إلى أحد المقدسات أو الشعائر المقررة في الأديان الأخرى متى كانت هذه المقدسات والشعائر مصونة وفقًا لأحكام الشريعة الإسلامية.

والابتزاز عبر الشبكة المعلوماتية التي اصبحت اجهزة الكمبيوتر والاتصالات توفر لها اسلوباً وموضوعاً جديداً فكثير من القضايا التي يشهدها العالم وتمثلت بصورة تهديد وابتزاز عبر الشبكات او داخل المؤسسات المجني عليها، ويتحقق ذلك من خلال الرسم والكتابه والقول وهذا ما تناولته المادة ٣٠٦ مكرر من قانون العقوبات المصري على تجريم كل من يتعرض للغير في مكان عام او خاص او مطروق باتيان امور او ايحاءات او تلميحات جنسية او اباحية سواء بالاشارة او القول او الفعل بأية وسيلة بما في ذلك وسائل الاتصالات السلكية او اللاسلكية.

وقد قررت المحكمة الاتحادية العليا بدولة الإمارات العربية المتحدة أنه: " من المقرر – في قضاء هذه المحكمة– أن لمحكمة الموضوع السلطة التامة في تكوين عقيدتها مما تطمئن إليه من أدلة الدعوى، ولها أن تأخذ باعتراف المتهم متى اطمأنت إليه لصدوره عن إرادة حرة وأن تستخلص من ذلك الاعتراف الصورة الصحيحة للواقعة ولا يشترط في الأدلة – ومنها الاعتراف – الذي اعتمدت عليه المحكمة في حكمها واتخذه سند لقضائها بالإدانة أن يُنبئ في كل جزئياته عن الواقعة بل للمحكمة أن تعضده بأدلة أو قرائن أخرى ذلك أن الأدلة في المواد الجنائية تكون متساندة يكمل بعضها بعضا بحيث تكون منها المحكمة مجتمعة عقيدتها ولا ينظر إلى الدليل بعينه دون باقي الأدلة بل يكفي أن تكون تلك

٣- سب أحد الأديان السماوية المعترف بها.

٤- تحسين المعاصي أو الحض عليها أو الترويج لها.

وإذا تضمنت الجريمة إساءة للذات الإلهية أو لذات الرسل والأنبياء أو كانت مناهضة للدين الإسلامي أو جرحًا للأسس والمبادئ التي يقوم عليها، أو ناهض أو جرح ما علم من شعائر وأحكام الدين الإسلامي بالضرورة، أو نال من الدين الإسلامي، أو بشر بغيره أو دعا إلى مذهب أو فكرة تنطوي على شيء مما تقدم أو حبذ لذلك أو روج له، فيعاقب بالسجن مدة لا تزيد على سبع (٧) سنوات". كما نصت المادة (٢٥) من القانون رقم (١٧٥) لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات المصري على أن: "يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامه لا تقل عن خمسين ألف جنية، ولا تجاوز مائة ألف جنية أو بإحدى هاتين العقوبتين، كل من اعتدى على أي من المبادئ أو القيم الأسرية في المجتمع المصري أو انتهك حرمة الحياة الخاصة، أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته أو منح بيانات شخصية إلى نظام أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقته أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات أو اخبارًا أو صور وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحه أم غير صحيحة".

(١) نصت المادة (١٧) من القانون الإماراتي رقم (٥) لسنة ٢٠١٢م بشأن مكافحة جرائم تقنية المعلومات على أنه: " يعاقب بالحبس والغرامة التي لا تقل عن مائتين وخمسن ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من أنشأ أو أدار موقعًا الكترونيًا أو أشرف عليه أو بث أو أرسل أو

نشر أو أعاد نشر عن طريق الشبكة المعلوماتية مواد إباحية أو أنشطة للقمار، وكل ما من شأنه المساس بالآداب العامة. يعاقب بالحبس والغرامة التي لا تقل عن مائتين وخمسن ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من أنشأ أو أدار موقعًا الكترونيًا أو أشرف عليه أو بث أو أرسل أو نشر أو أعاد نشر عن طريق الشبكة المعلوماتية مواد إباحية أو أنشطة للقمار، وكل ما من شأنه المساس بالآداب العامة". كما نصت المادة (٢٦) من القانون رقم (١٧٥) لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات المصري على أن: "يعاقب بالحبس مدة لا تقل عن سنتين، ولا تجاوز خمس سنوات، وبغرامة لا تقل عن مائة ألف جنية لاتجاوز ثلاثة مائة الف جنية، أو بإحدى هاتين العقوبتين، كل من تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها بمحتوى مناف للآداب العامه، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفة".

الأدلة في مجموعها مؤدية إلى ما قصده الحكم منها تتجه في اكتمال اقتناع المحكمة واطمئنانها إلى ما انتهت إليه من نتيجة، وكان من المقرر – أن القصد الجنائي أمر يضمره الجاني في خبيئات نفسه ولا يمكن الاستدلال عليه أو استخلاصه إلا من خلال الشواهد الخارجية المحيطة بالوقائع المصاحبة لها، وأن استخلاص هذا القصد من المسائل الموضوعية التي تستقل بها محكمة الموضوع بغير معقب عليها في ذلك طالما كان استخلاصها سائغا ومقبولا ومستمدا مما له أصله الثابت بالأوراق وأن المحكمة غير ملزمة بالتحدث استقلالا عن القصد الجنائي إذ يكفي أن يشير إليه الحكم ضمنا عند تحصيله لوقائع الدعوى أو تقديرها لأدلتها لما كان ذلك وكان الثابت من مدونات الحكم الابتدائي المؤيدة أسبابه بأسباب الحكم المطعون فيه أنه قد عرض لواقعة الدعوى وأحاط بظروفها وأدلتها عن بصر وبصيرة وأدان الطاعن عن التهمتين المسندتين إليه أخذا مما اطمأن إليه من اعتراف المتهم وما جاء بمحضر الضبط والمسطر في مدوناته بمقولة "وكانت المحكمة تطمئن لثبوت التهمتين المسندتين للمتهم أخذا من إقرار المتهم ..... في جميع مراحل الدعوى ... بأنه كان يحوز على صور أطفال صغار السن وهم عرايا ويمارسون الجنس وكان محتفظ بها بجهاز الحاسوب الخاص به وشريحة المموري كارت والذي عضد ذلك ما جاء بتقرير أفراد الضبط بأنه من خلال قيام إحدى الدوريات الإلكترونية بإدارة المباحث الإلكترونية تم رصد مجموعة من الأشخاص يحوزون على ملفات جنسية لأطفال ويقومون بنشرها في الشبكة الإلكترونية"[1]. ويفهم من هذا الحكم صرامة المشرع الإماراتي في التصدي للجرائم الإلكترونية على وجه العموم، وما يؤدي منها إلى نشر الرذيلة والإضرار العام بالمجتمع ومصالح الدولة على وجه الخصوص، فلم تستخدم المحكمة أحكام الرأفة في مثل هذه الجرائم، وذلك لخطورتها على المجتمع.

وما نراه ايضاً هو ان المواقع الجنسية تنتشر عبر شبكات الانترنت واخذت هذه المواقع بالزيادة مما يؤثر سلباً على المجتمع فمن اخطر الجرائم الجنسية االلكترونية ظهور الاباحية والخلاعه على الانترنت وغرف الدردشة ومجموعات الاخبار والبريد االلكتروني التي تتناول عرض الافلام الاباحية والصور الخلاعية التي تتعلق بالاطفال فظهرت دعارة الاطفال على الانترنت في امريكا سنة ١٩٩٥ وكان للكونغرس الامريكي تنظيم اوجه الاباحية والاطفال عبر الانترنت فاصدر قانون الاداب للاتصالات (CDA) سنة ١٩٩٦[2]، وبعد هذا العرض لبعض من صور الجرائم الكمبيوتر فإننا نصل إلى أن اي وصف منها لم يكن شاملًا لكافة جرائم الكمبيوتر وذلك لحداثة هذا النوع من الجرائم نسبياً مقارنة مع باقي الجرائم التقليدية كالسرقة والقتل والاغتصاب ونظراً للتطور السريع والمتواصل فيمكن لهذا النوع من الجرائم مما يضيف انماطًا وصور اخرى للجرائم االلكترونيةـــ، غير أن القضاء استبعد وصف

---

(١) دولة الإمارات العربية المتحدة: المحكمة الإتحادية العليا – الأحكام الجزائية – الطعن رقم ٤١٦ لسنة ٢٠١٤ قضائية بتاريخ: ٢-٢-٢٠١٥م.

(٢) محمد الأمين الشوابكه، جرائم الحاسوب والانترنت الجريمة المعلوماتية، مرجع سابق، ص١٢٠.

جريمة سرقة بخصوص تقليد تلك البرامج لانتفاء حق المسئول ، ولعدم تكرار ارتكبه الاختلاس ولن أعملت الحماية الواردة بنص خاص تضمنه قانون حماية حق المؤلف [١] .

المبحث الثاني

الأساس القانوني لجريمة اختراق المواقع الرسمية غي القوانين الإماراتية والمقارنة

تمهيد وتقسيم:

تعد فكرة استخدام آلة (كمبيوتر) في معالجة الأرقام ليست بالجديدة[٢]؛ حيث أشار بعض الباحثين إلى استخدام مثل هذه الوسيلة – في صورتها الأولى – وجد في آسيا منذ خمسة آلاف عام[٣]، كما مهدت الثورة الصناعية، منذ منتصف القرن الماضي ومن خلال التقدم التقني في مجال الحواسيب الآلية، لبزوغ ثورة جديدة هي ثورة المعلومات، وما أدت إليه من جرائم إلكترونية[٤]، وبات الأمر واضحاً أن القرن الحادي والعشرين، هو قرن المعلومات (Le siécle de l'information) واستحداث أجهزة تسمح بمعالجة هذه المعلومات هو ركيزة هذه الثورة الهائلة[٥]. وقد ذهب بعض الفقه إلي القول بإمكانية إخضاع النصوص العقابية التقليدية الخاصة ببعض الجرائم، كجريمة السرقة وجريمة خيانة الأمانة، وجريمة دخول ملك الغير على، اختراق جريمة الدخول بغير وجه حق، ألا أن هذه المحاولة لم تكتب لها النجاح لما فيها من تشويه المبادئ المستقر عليها، والتي تقوم عليها هذه الجرائم؛ حيث إن النصوص التقليدية لا تؤمن الحماية الكافية للمال المعلوماتي؛ والذي يختلف بطبيعته عن المال التقليدي والقول بغير ذلك، يؤدي إلى ثغرة في نظام حماية الأموال المعلوماتية، فقد تتشابه جريمة الدخول بغير وجه حق إلى النظم المعلوماتية مع بعض الجرائم التقليدية، مثل جريمة السرقة وجريمة دخول ملك الغير. ومع ذلك، فإن لجريمة اختراق المواقع الرسمية، أساسها القانوني في التشريعات الإماراتية والمقارنة، وهو ما سوف نتعرض له في مطلبين على النحو التالي:

المطلب الأول: اختراق المواقع الرسمية في القوانين الإماراتية.

المطلب الثاني: اختراق المواقع الرسمية في القوانين المقارنة.

---

(1) Michel vivant et autres , Droit de l'informatique et des réseaux , Lamy , 2001 , p. 1837 .

(٢) سعيد عبد اللطيف حسن: إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، ط١، بدون دار طبع، ١٩٩٩م، ص١٣.

(3) Walsh (John) , Standard Grade – Computing Studies – 1994. pp. 308. Bill Gates , The Road Ahead 1995 p. 93 – 99.

(٤) علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديدة للنشر، الإسكندرية، ١٩٩٧م، ص١.

(٥) محمد سامي الشوا: ثورة المعلومات وانعكاساتها علي قانون العقوبات، دار النهضة العربية، القاهرة، ٢٠٠٣م، ص١٧.

المطلب الأول
اختراق المواقع الرسمية في القوانين الإماراتية

تمهيد وتقسيم:

انطلقت في العاصمة الإماراتية أبوظبي، الإثنين ١٥ مايو ٢٠١٧م، الأعمال المتعلقة بالمؤتمر الدولي لتجريم الإرهاب الإلكتروني، والذي استمر لمدة يومين بقصد إيجاد أرضية قانونية دولية مشتركة تتصدى لظاهرة الإرهاب في الفضاء الرقمي، وقد أكد وزير الدولة الإماراتي للشؤون الخارجية في الكلمة الافتتاحية التي ألقاها في المؤتمر على أهمية المؤتمر والقضية التي يطرحها، والمعنية بمكافحة الإرهاب الإلكتروني، حسبما أفادت وكالة الأنباء الإماراتية، وقد شارك في المؤتمر الدولي لتجريم الإرهاب الإلكتروني نخبة من أصحاب القرار والخبراء المتخصصين في القانون والجرائم الإلكترونية ومكافحتها، من مختلف دول العالم، وقد ناقشت جلسات المؤتمر الدولي أنجع السبل لردم الهوة القانونية والتشريعية في تنظيم الفضاء الإلكتروني؛ حيث أصبح الجرائم الإلكترونية خطراً يهدد العالم بأسره، وهاجساً يخيف العالم الذي بات عرضة لهجمات القراصنة والمخترقين للمواقع الرسمية، عبر الإنترنت، الذين يمارسون نشاطهم التخريبي من أي مكان في العالم(١).

ولقد تزايدت مخاطر الجرائم الإلكترونية في الآونة الأخيرة، وعلى وجه التحديد منذ بزوغ فجر الثورة التكنولوجية وما أفرزته من آثار سلبية نجم عنها ظهور جريمة جديدة غير معروفة؛ ألا وهي جريمة اختراق المواقع الإلكترونية؛ حيث يعد هذا النوع من الجرائم، أشد خطراً وأعظم ضرراً من الجرائم التقليدية، وعلى وجه الخصوص في مستواها الفني والتقني التي يتميز بها المجرم الإلكتروني، وذلك في مجال استخدام تكنولوجيا المعلومات والبيانات؛ ومن حيث أدوات ارتكاب جريمة الإلكترونية، أو النطاق الزماني والمكاني لهذه الجريمة، واعتبارها من الجرائم العابرة للوطنية في العديد من صورها، وهو ما يقلل من وسائل وأساليب وإمكانات وقدرات التصدي لها ومواجهتها في العديد من الحالات، وعلى هذا الأساس، وفي ضوء ما شهدته دولة الإمارات العربية المتحدة، باعتبارها من دول العالم الرائدة على المستويين: الإقليمي والدولي، وذلك في تنامي استعمال التقنيات والإلكترونيات في العديد من المجالات، مع تزايد استخدام التطبيقات الإلكترونية، إلى الحد الذي صارت معه الحياة تعتمد بشكل عام في غالبية مؤسساتها: العامة والخاصة، وفي شتى مناحي الحياة، على النظم والوسائل الإلكترونية، وهو ما أدى إلى تزايد خطر الجرائم الإلكترونية، في ظل الاستخدام المتزايد لأدوات

---

(١) خبر متاح عبر الرابط الإلكتروني: https://www.skynewsarabia.com

ووسائل التقنية الرقمية، وفي مواجهة هذه الجرائم، فقد قام المشرع الإماراتي بإصدار العديد من التشريعات الملائمة لمواجهة الجرائم الإلكترونية وكيفية للتعامل معها، وذلك بقصد حماية المجتمع الإماراتي من مخاطرها وتهديداتها[١] .

وتعد الجرائم الإلكترونية، وعلى وجه الخصوص جريمة اختراق المواقع الرسمية – على حد قول أحد خبراء مكتب الأمم المتحدة لمكافحة الجريمة – هي جريمة الأجيال القادمة، وعلى ذلك يجب أن تتضافر كافة الجهود الدولية لمكافحة جريمة اختراق المواقع الرسمية، وهو ما سارع إليه مجلس التعاون الخليجي، وذلك بوضع القوانين الخاصة للتصدي لهذه الجريمة، ومن الأمثلة على ذلك، ما قامت – وما زالت تقوم – به دولة الإمارات العربية المتحدة، وذلك بسن التشريعات الخاصة بمكافحة جرائم الإنترنت، بمختلف أنماطها وشتى صورها، فأصدرت في سبيل ذلك عدة قوانين، منها: القانون رقم (١) لسنة ٢٠٠٦م بشأن المعاملات والتجارة الإلكترونية[٢]. وهو ما نبينه في ثلاثة فروع على النحو الآتي:

الفرع الأول: أساس الجرائم الإلكترونية في التشريع الإماراتي

بادر المشرع الإماراتي بإصدار القانون الاتحادي رقم (٢) لسنة ٢٠٠٦م، في شأن مكافحة جرائم تقنية المعلومات[٣]، وقد تضمن هذا القانون تعريفًا للمعلومات الإلكترونية، وكذلك تعريفًا لمفهوم البرنامج المعلوماتي، وغير ذلك من نظام المعلومات الإلكترونية، والشبكات المعلوماتية، والمستندات الإلكترونية التابعة للمواقع الإلكترونية، وكذلك وسيلة تقنية المعلومات والبيانات الحكومية.

كما تضمّن القانون في العديد من مواده المتنوعة تحديداً للأفعال التي من شأنها أن تشكل خطراً وضرراً لنظم التقنية المستخدمة وأدواتها المختلفة، كما تضمن تحديد العقوبات التي تتعلق بارتكاب أيٍّ من هذه الأفعال، ومن أمثلة هذه الصور أو الأفعال، التي تضمنها هذا القانون، ما يلي[٤]:

(١) الوصول بوجه غير مشروع إلى أيّ موقع أو نظام من المواقع والأنظمة المعلوماتية[٥].

---

(١) محمد أحمد محمد الحمادي، تشريعات مكافحة جرائم تقنية المعلومات في دولة الإمارات وأحكام القضاء، دولة الإمارات العربية المتحدة، أبوظبي، شرطة أبوظبي، مركز الدراسات الأمنية، ورقة عمل قدمها الباحث في ندوة شبكات الإنترنت وتأثيراتها الاجتماعية والأمنية، ط٢، في الفترة من (٦–٧) من شهر نوفمبر لعام ٢٠٠٦م، ص٩.

(٢) صدر هذا القانون في قصر الرئاسة بمدينة أبو ظبي، بتاريخ ٣٠ ذي الحجة ١٤٢٦هـ، الموافق ٣٠ يناير ٢٠٠٦م.

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

(٤) القانون الاتحادي الإماراتي رقم (٢) لسنة ٢٠٠٦م في شأن مكافحة الجرائم الإلكترونية وتعديلاته بالقانون رقم (٥) لسنة ٢٠١٢م.

(٥) انظر: الفقرة رقم (١) من المادة (٢) من هذا القانون.

(٢) إلغاء أو حذف أو تدمير أو إنشاء أو إتلاف أو تغيير أو إعادة نشر للبيانات والمعلومات التي يحتويها الموقع أو النظام المعلوماتي[١].

(٣) تزوير المستندات الإلكترونية الحكومية، سواء الاتحادية أو المحلية، أو الهيئات أو المؤسسات العامة الاتحادية والمحلية[٢].

(٤) استعمال المستند الإلكتروني المزور، مع علمه بواقعة التزوير[٣].

(٥) تعطيل أو إعاقة الوصول إلى الخدمات الإلكترونية أو الأجهزة والبرامج ومصادر البيانات والمعلومات بأية وسيلة كانت هذه الإعاقة[٤].

(٦) تعطيل أو إيقاف أو تدمير أو حذف أو مسح أو إتلاف محتويات شبكة المعلومات أو البيانات أو إحدى وسائل تقنية المعلومات[٥].

(٧) استخدام شبكة المعلومات لأهداف يقصد بها تهديد وابتزاز الأشخاص أو الاستيلاء على وسيلة من وسائل تقنية المعلومات[٦].

(٨) وتستخدم شبكة المعلومات الدولية أو أية وسيلة من وسائل تقنية المعلومات، بقصد للوصول غير المشروع إلى قاعدة البيانات والأرقام التي تخص بطاقة أو أكثر من البطاقات الائتمانية[٧].

(٩) كما تستخدم شبكة المعلومات الدولية أو أية وسيلة من وسائل تقنية المعلومات، بغرض الإساءة إلى شعيرة من شعائر الإسلام، أو الإساءة أو السخرية من أحد المقدسات الدينية[٨]، وفي ذلك قضت المحكمة الاتحادية العليا بأنه: يجب الحكم بغرامة لا تجاوز حدها الأقصى الوارد بالفقرة الأولى من المادة (٢٠) من المرسوم بقانون رقم ٥ لسنة ٢٠١٢م أو بمبلغ لا يقل عن حدها الأدنى الوارد في المادة نفسها، وذلك في جرائم القذف الإلكتروني[٩].

ومما تجدر الإشارة إليه أن هذا القانون قد تضمن الإشارة إلى العديد من صور اختراق المواقع الرسمية غير ما ذكر، بيد أننا اكتفينا بالإشارة إلى أهم الصور وأبرزها.

---

(١) انظر: الفقرة رقم (٢) من المادة (٢) من هذا القانون.

(٢) انظر: الفقرة الأولى من المادة (٤) من هذا القانون.

(٣) انظر: الفقرة الثالثة من المادة (٤) من هذا القانون.

(٤) انظر: المادة (٥) من هذا القانون.

(٥) انظر: المادة (٦) من هذا القانون.

(٦) انظر: المادة (٩) من هذا القانون.

(٧) انظر: المادة (١١) من هذا القانون.

(٨) انظر: المادة (١٥) من هذا القانون.

(٩) المحكمة الاتحادية العليا، دائرة الأحكام الجزائية، الطعن رقم ٤٩٣، لسنة ٢٠١٤ قضائية، بتاريخ ٢٠١٥/٤/٢٧م.

وعلى ذلك فإن المشرع الإماراتي قد بين على وجه الدقة، وحدد العقوبات، التي يجب أن تطبق على من يرتكب أي فعل من الأفعال سابقة البيان، أو غيرها من الجرائم الوارد ذكرها في القانون، وقد تمثلت هذه العقوبات في الحبس والغرامة والسجن المؤقت، كما نص القانون على بعض العقوبات الفرعية التي تتمثل في الإبعاد للجاني الأجنبي، ومن الملاحظ أن المشرع الإماراتي في هذا القانون، لم يهمل تجريم الأفعال التي فيها مساس بنظم التقنية، أو الأدوات التي تستخدم فيها، بل حدد المشرع هذه الأفعال، ونص على العقوبات المقرر لمن يرتكبها(١).

ومن هذه الصور ما قضت به المحكمة الاتحادية العليا(٢): بمعاقبة إرهابيين إلكترونيين؛ حيث قضت وطلبت معاقبتهما بما ورد في القانون الاتحادي رقم (٧) لسنة ٢٠١٤م في شأن مكافحة الجرائم الارهابية؛ حيث نسبت إليهما المحكمة تهمة ارتكاب جريمة إرهابية إلكترونية، وذلك بانضمامهما إلى تنظيمات وجماعات وميليشيات إرهابية، والترويج لأفكارها عبر الإنترنت(٣)، وكذلك ما قضت به ذات المحكمة، بسريان أحكام هذا القانون في شأن جريمة السب والقذف باستخدام الشبكة المعلوماتية(٤).

الفرع الثاني: القوانين المتعلقة بالجرائم الإلكترونية

أجرى المشرع الإماراتي العديد من التعديلات على التشريعات المتعلقة بالجرائم الإلكترونية، فلم يقف المشرع الإماراتي مكتوف الأيدي تجاه ما يحدث من تطورات في النظم المعلوماتية، ولم يتوقف عند إصدار القانون رقم (٢) لسنة ٢٠٠٦م السالف الذكر والبيان، بل قام المشرع بإصدار القانون الاتحادي رقم (٥) لسنة ٢٠١٢م، والخاص بمكافحة الجرائم الإلكترونية، وكان المشرع يقصد بذلك مواكبة ومسايرة المستجدات والمتغيرات في مجال التقنية الرقمية، سواء ما كان منها على الساحة المحلية أم الإقليمية أم الدولية في هذا المضمار، ومن أجل ذلك، فقد قام المشرع الإماراتي بالعديد من الإضافات والتعديلات على القانون رقم (٢) لسنة ٢٠٠٦م، في شأن مكافحة جرائم تقنية المعلومات، وفيما يلي نبين أهم هذه التعديلات والإضافات، وذلك على النحو التالي:

(١) لقد اشتملت نصوص القانون الجديد على الأفعال الخاصة بجرائم الاختراق الإلكتروني، وجرائم المعاملات والتجارة الإلكترونية، وكذلك جريمة الاتجار بالبشر، فضلًا عن جرائم الآثار، وحيازة المتفجرات والذخائر والأسلحة النارية، وتهديد الأمن الإلكتروني، وكلها جرائم لم يوردها المشرع الإماراتي في القانون القديم الذي تم إصداره سنة ٢٠٠٦م، وكان الغرض من وراء

---

(١) جاء النص على عقوبة كل جريمة في هذا القانون عند ذكرها في الموضع المخصص لها.

(٢) المحكمة الإتحادية العليا، دائرة الأحكام الجزائية، الطعن رقم ١، لسنة ٢٠١٥ قضائية، بتاريخ ٢٠١٥/٦/١٦م.

(٣) الحكم متاح على شبكة قوانين الشرق عبر الرابط الإلكتروني:http://site.eastlaws.com.

(٤) المحكمة الاتحادية العليا، دائرة الأحكام الجزائية، الطعن رقم ٤٨٣، لسنة ٢٠١٦ قضائية، بتاريخ ٢٠١٦/١٢/٩م.

إصدار هذه التعديلات مسايرة المستجدات والمتغيرات، وغيرها من صور الجرائم المستحدثة، وكافة الأنشطة المالية والتجارية المتنوعة والأمن المعلوماتي[١].

(٢) كما اشتملت مواد هذا القانون على بعض التعريفات الجديدة، التي خلا القانون القديم من ذكرها؛ حيث عرّف هذا القانون المنشآت المالية أو التجارية أو الاقتصادية، مع بيان مصطلح إلكتروني، والمواد الإباحية والأحداث، والعنوان البروتوكولي لشبكة المعلومات الدولية، وغيرها من المصطلحات والألفاظ ذات الصلة، وقصد المشرع من وراء إيراد هذه التعريفات احتواء القانون على جميع صور وأشكال الأنشطة الإلكترونية غير المصرح بها، وتأمين ما يتم ممارسته من الأعمال التجارية الإلكترونية بواسطة النظم التقنية؛ حتى لا تتعرض لسطو المجرمين الإلكترونيين[٢].

(٣) سلك المشرع الإماراتي – في هذا القانون – مسلك التغليظ في فرض العقوبات السالبة للحرية (السجن والحبس)، مع ارتفاع القيمة المالية في عقوبة الغرامة، كما نص المشرع الإماراتي على بعض من العقوبات الفرعية والعقوبات التكميلية، وكذلك التدابير الاحترازية، وذلك بمقتضى القانون الجديد، والأمر على خلاف ذلك في القانون السابق؛ ومن مظاهر تغليظ العقوبة في هذا القانون النص على عقوبة السجن المؤبد، وهو ما لم يكن كذلك في القانون القديم، وكذا النص على الجزاء على الشروع، بعقاب يعادل نصف عقوبة الجريمة التامة في مواد الجنح، وذلك طبقًا لنص المادة (٤٠) منه[٣]، وهو ما خلا القانون القديم من النص عليه.

(٤) وفيما يتعلق بعقوبة الغرامة، والتي كانت لا تزيد عن مائتي ألف درهم بالقانون القديم، فقد وصلت قيمتها إلى ثلاثة ملايين درهم، طبقًا لأحكام القانون الجديد[٤].

(٥) كما نص المشرع في القانون الجديد على اعتبار جرائم الاختراق الإلكتروني، وجرائم تقنية المعلومات والبيانات، من الجرائم الماسة بأمن الدولة[٥]، وذلك في إشارة من المشرع إلى بيان خطورة هذه الجرائم على أمن وأمان والمجتمع وسلامته[٦].

---

(١) انظر في ذلك: المواد (٢٣ – ٢٥ – ٣٣) من القانون المذكور.

(٢) عبيد صالح حسن، سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية، مجلة الفكر الشرطي، المجلد رقم (٢٤) – العدد رقم (٩٥) أكتوبر، ٢٠١٥م، ص٤٥.

(٣) حيث تنص هذه المادة على أنه: "يعاقب على الشروع في الجنح المنصوص عليها في هذا المرسوم بقانون بنصف العقوبة المقررة للجريمة التامة".

(٤) انظر المادة (١٠) من هذا القانون.

(٥) حيث نصت المادة (٤٤) من هذا القانون على أنه: "تعتبر الجرائم الواردة في المواد (٤، ٢٤، ٢٦، ٢٨، ٢٩، ٣٠، ٣٨) من هذا المرسوم بقانون من الجرائم الماسة بأمن الدولة. كما تعتبر من الجرائم الماسة بأمن الدولة، أي جريمة منصوص عليها في هذا المرسوم بقانون إذا ارتكبت لحساب أو لمصلحة دولة أجنبية أو أي جماعة إرهابية أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة".

(٦) عبيد صالح حسن، سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية، ص٤٦.

(٦) كما اعتبر المشرع – في هذا القانون الجديد – بعض صور الجرائم، أو بعض السلوكيات أو الأفعال، أو تكرار ارتكابها ظرفًا من الظروف المشددة، وهو ما يعني ضرورة تغليظ العقوبة في حق مرتكب هذه الجرائم، أو ممارسة هذه الأفعال أو تلك السلوكيات[١].

(٧) أنشأ المشرع عقوبة جديدة من العقوبات الفرعية – غير المصادرة والإغلاق الكلي أو الجزئي للموقع أو محل الجريمة – وهي عقوبة الإبعاد بالنسبة للأجنبي عند ارتكابه لفعل من الأفعال المنصوص عليها في هذا القانون الجديد[٢].

(٨) كما أورد المشرع في القانون الجديد بعض التدابير الاحترازية، التي توقع في حق مرتكبي فعل أو أكثر من الأفعال المنصوص عليها في القانون، وتمثلت هذه التدابير الاحترازية في الحرمان، أو الرقابة أو الإشراف، أو الإيداع في مركز تأهيل أو مأوى علاجي[٣].

(٩) ورغم ما اتسم به هذا القانون من تغليظ العقوبات، فقد نص على تخفيف العقوبة أو الإعفاء منها، في الحالة التي يتم فيها الإبلاغ عنها، وذلك بقصد تحفيز مرتكب هذه الجرائم، أو من كانت بحوزته معلومات بشأن هذه الجرائم، للإبلاغ عنها لمنع وقوعها أو كشف من ينوي ارتكابها، ومن ثم ملاحقتهم والقبض عليهم حال ارتكابها[٤].

ونلاحظ: من خلال العرض السابق، أن المشرع الإماراتي قد تدرج في العقوبات، وكأنه يعطي إشارة للمجرم الإلكتروني بمثابة إنذار وتحذير، أن عُدْ إلى رشدك، وإلا فإن العقوبة رادعة والجزاء كافٍ لزجرك، كما أن هذا التدرج العقابي مناسب للطبيعة البشرية، ويحقق العدالة في تطبيق العقوبات.

الفرع الثالث: اختراق المواقع الإلكترونية في القانون الجديد رقم (٥) لسنة ٢٠١٢م

القانون الجديد رقم (٥) لسنة ٢٠١٢م بشأن مكافحة جرائم تقنية المعلومات(٥)، هو تعديل للقانون رقم (٢) لسنة ٢٠٠٦م بشأن مكافحة جرائم تقنية المعلومات، وتتبين سياسة المشرع الإماراتي في محاربة جريمة اختراق المواقع الإلكترونية والتصدي لها، طبقًا لأحكام هذا القانون من خلال ما يلي:

(١) في هذا القانون سلك المشرع الإماراتي مسلك التجريم والعقاب، على الأعمال التي تتعلق بجرائم اختراق المواقع الإلكترونية والمعاملات والتجارة الإلكترونية، وكذلك جرائم

---

(١) انظر في ذلك: المادة (٤٦) من هذا القانون.

(٢) انظر في ذلك: المادة (٤٢) من هذا القانون، وسيأتي تفصيل ذلك في فصل العقوبات.

(٣) انظر في ذلك: المادة (٤٣) من هذا القانون.

(٤) انظر في ذلك: المادة (٤٥) من هذا القانون.

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

الاتجار بالبشر، وأيضاً الجرائم ذات الصلة بالآثار والسياحة والمتفجرات والذخائر والأسلحة النارية، وكافة الجرائم المتعلقة بمجال بالأمن الإلكتروني[١].

(٢) وفي سبيل تحقيق المزيد من الحماية للفضاء الإلكتروني، فقد أضاف المشرع الإماراتي، صياغة جديدة لبعض التعريفات، مثل: مصطلح "إلكتروني"، ومفردات "المنشآت المالية والتجارية والاقتصادية"، وكذلك مصطلح "مواد إباحية"، والعنوان البروتوكولي للإنترنت، إلى غير ذلك من المصطلحات التي تبين مقصد المشرع في محاربته لكافة صور اختراق المواقع الإلكترونية، كما اعتبر المشرع أن جريمة السب بوسيلة إلكترونية، تخضع لأحكام هذا القانون، وفي ذلك قضت المحكم الاتحادية العليا، بأن السب عبر البريد الإلكتروني مجرّم بمقتضى هذا القانون[٢]، كما نص المشرع الإماراتي في هذا القانون على العقاب الذي قد يصل إلى حد السجن المؤبد، لمن يرتكب أيًا من الجرائم المنصوص عليها، ومنها: جريمة اختراق المواقع الإلكترونية.

(٣) نص المشرع الإماراتي في هذا القانون على معاقبة الشروع في الجريمة بنصف عقوبة الجريمة التامة في الجنح.

(٤) زاد المشرع الإماراتي في هذا القانون قيمة الغرامة المالية كعقوبة، والتي قد تصل إلى ثلاثة ملايين درهم، في بعض الأفعال والسلوكيات، المجرمة بنصوص القانون.

(٥) ذهب المشرع إلى اعتبار بعض الأفعال أو السلوكيات، التي تتعلق بالجرائم الإلكترونية، من الجرائم الخطرة التي تتعلق بأمن وسلامة الدولة.

(٦) كما اعتبر المشرع الإماراتي في هذا القانون، أن أي جريمة ورد النص عليها، هي من الجرائم الماسة بأمن الدولة، وذلك في الحالات التي ترتكب فيها هذه الجرائم لصالح أو لمصلحة وحساب دولة أجنبية أو جماعة إرهابية أو جمعية أو مجموعة أو منظمة أو هيئة غير مشروعة.

(٧) كما نص المشرع الإماراتي على أن بعض الأفعال أو السلوكيات التقنية، يمكن اعتبارها من الظروف المشددة التي تستوجب تغليظ العقوبة في بعض الحالات.

(٨) كما نص المشرع على عقوبة الإبعاد للأجنبي كعقوبة تبعية جديدة، وذلك في الحالة التي يرتكب فيها فعلًا أو سلوكًا ورد النص على تجريمه بمقتضى هذا القانون، وهو بذلك غير المصادرة والإغلاق الكلي أو الجزئي للمحل أو الموقع.

---

(١) عبيد صالح حسن، سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية، مرجع سابق، ص٤٦.

(٢) المحكمة الاتحادية العليا، دائرة الأحكام المدنية والتجار، الطعن رقم ١، لسنة ٢٠١٥ قضائية، بتاريخ ٢٠١٥/٦/١٦م.

(٩) كذلك نص المشرع على بعض التدابير الاحترازية، التي توقع على من يرتكب الأفعال والسلوكيات المجرمة بموجب أحكام هذا القانون، ومن هذه التدابير: الرقابة والإشراف، والحرمان، وتأهيله في أحد مراكز التأهيل أو إيداعه في مستشفى طبي، وذلك فضلًا عن العقوبات الأصلية للجريمة والعقوبات الفرعية أو التكميلية لها.

(١٠) كما انتهج المشرع الإماراتي في هذا القانون منهج التخفيف في بعض العقوبات أو الإعفاء منها بصفة نهائية، شريطة القيام بالإبلاغ عن الفعل أو السلوك الذي تم النص عليه في القانون، وذلك قبل اكتشافه أو اكتشاف المجرم، للمساعدة في التوصل إليهم والقبض عليهم قبل ارتكاب الجريمة.

ونرى: أن المشرع الإماراتي قد تصدى لجريمة اختراق المواقع الإلكترونية، ليس على المستوى الأمني فحسب، بل على المستوى الثقافي والاجتماعي، وذلك من خلال العديد من الإصدارات والدوريات، التي تهدف إلى توعية المجتمع بخطر الجرائم الإلكترونية، ولا ينسى الدور المهم الذي تلعبه أكاديمية شرطة دبي[١] في التصدي لخطر اختراق المواقع الإلكترونية، فضلًا عما يقوم به مركز الإمارات للدراسات والبحوث الاستراتيجية[٢]؛ حيث أصدر المركز العديد من الرسائل والكتب والإصدارات في بيان مفهوم الجرائم الإلكترونية، بكافة صورها وأشكالها والتصدي لها على كافة المستويات.

المطلب الثاني

اختراق المواقع الإلكترونية في القوانين المقارنة

تمهيد وتقسيم:

---

(١) التعريف بالأكاديمية: "أنشئت كلية شرطة دبي عام ١٩٨٧م بمقتضى القانون رقم (١) لسنة ١٩٨٧م، وبدأت الدراسة رسميًا في التاسع عشر من سبتمبر لعام ١٩٨٧م، انطلاقًا من مدرسة تدريب الشرطة بإدارة الطوارئ في حينه، إلى أن اكتمل مبنى الأكاديمية في شكله الحالي، واكتملت البنية الأساسية للكلية في شهر أكتوبر من عام ١٩٨٨م بعد إصدار القرار رقم (١) لسنة ١٩٨٨ في شأن اللائحة الداخلية لكلية الشرطة، وافتتحـــــت الكلية رسميـــــًا في الأول من أبريل عام ١٩٨٩م ".

https://www.dubaipolice.ac.ae.

(٢) التعريف بالمركز: هو مؤسسة بحثية مستقلة ومتطورة، لا يقتصر دورها على مواكبة آخر التطورات والمستجدات على الصعيد السياسي والاقتصادي والاجتماعي فحسب، وإنما تسعى جاهدة إلى صياغة الاستراتيجيات الملائمة لوضع المجتمع الإماراتي في مكان لائق ومنزلة سامية، في خضم سباق الحداثة، وقد تم إنشاء المركز عام ١٩٩٤م ليبقى دومًا صرحاً فريداً من نوعه في منطقة الشرق الأوسط؛ حيث أرسى المركز منذ نشأته العديد من معايير التميز والكفاءة في الدراسات والبحوث الاستراتيجية.

http://www.ecssr.com.

التزايد في معدل الحوادث الإلكترونية ما هو إلا بسبب دخول الإنترنت، وعلى وجه الخصوص اختراق المواقع الإلكترونية، وغير ذلك من الجرائم غير العمدية والتي تزايدت زيادة مضطردة[١].

وبالنظر إلى ما يمثله اختراق المواقع الإلكترونية من أخطار، فقد أدرك العالم ضرورة التعاون الدولي فيما بين الدول بقصد تجاوز تحديات الجرائم الإلكترونية، فلجأ البعض إلى عقد الاتفاقيات والمعاهدات الثنائية، التي تهدف إلى التعاون المشترك لتيسير مهمة التحقيق في الجرائم الإلكترونية[٢]. وفي سبيل ذلك سعت بعض الدول – العربية وغير العربية – إلى سن التشريعات ووضع القوانين، لمكافحة ظاهرة اختراق المواقع الإلكترونية، كما سارع البعض إلى تطوير وتكثيف سياساته الأمنية والتقنية، والتي من شأنها صعوبة اختراق أنظمة وشبكات الاتصالات، بينما اتجه البعض إلى التصدي للفساد الذي يؤدي إلى اختراق المواقع الإلكترونية؛ ومن ثم التطوير لصناعة تقنية الاتصالات والمعلومات، ودعم أمن البلاد الوطني، وركزت بعض الدول إلى إقامة المؤتمرات وعقد الندوات المتخصصة، ودعوة أصحاب الأفكار للحديث عن هذه الظاهرة، وما يهمنا في هذا المقام، هو التصدي قانونياً لجريمة اختراق المواقع الإلكترونية، وموقف التشريعات المقارنة منها، سواء كان ذلك على المستوى العربي أو الأجنبي أو الدولي، وفي ضوء ذلك نقسم هذا المبحث إلى ثلاثة فروع وذلك على النحو التالي:

الفرع الأول: اختراق المواقع الإلكترونية في القوانين العربية

تباينت نظرة القوانين العربية في تشريعاتها حيال ظاهرة اختراق المواقع الإلكترونية، وفي ضوء ذلك نتناول بإيجاز اختراق المواقع الإلكترونية في بعض القوانين العربية، وذلك على النحو التالي:

أولًا – اختراق المواقع الإلكترونية في القوانين المصرية: تعمل وزارة الاتصالات والمعلومات المصرية – الآن – على إصدار نظام لضبط الجريمة الإلكترونية؛ حيث يتضمن هذا النظام العقوبات الرادعة، ضد من يسعى من الأفراد أو المؤسسات إلى تزوير أو إفساد أو تعطيل المستندات الإلكترونية على شبكة المعلومات الدولية، أو مجرد محاولة الكشف عن البيانات والمعلومات التي لا تخصه بدون وجه حق، وغير ذلك من صور الجريمة الإلكترونية، بما في ذلك جريمة اختراق المواقع الإلكترونية وتعقب المجرمين الإلكترونيين.

---

(1)Bouzat. J. pinatel. Traité ole droit penal et de Criminologie. Toml Droit penal , Paris.

(٢) حسن طاهر داوود، جرائم نظم المعلومات، ط١، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٠م، ص٢٠٩؛ محمد الأمين البشري، بحث بعنوان: التحقيق في جرائم الحاسب الآلي، مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، الذي تم انعقاده في كلية الشريعة والقانون بدولة الإمارات العربية المتحدة، في الفترة من الأول إلى الثالث من شهر مايو لعام ٢٠٠٠م، ص٧٨.

وفي بداية شهر أكتوبر ٢٠١٧م، بدأ البرلمان المصري مناقشة قانون يهدف إلى مكافحة الجريمة الإلكترونية؛ وذلك بقصد محاربة العنف والجرائم الإلكترونية، والتصدي لصفحات ومواقع الإنترنت، وقد عرض مجلس النواب هذا القانون للمناقشة خلال الفترة الماضية، وتجري الآن صياغته من قِبل اللجنة التشريعية للاتفاق النهائي على مواد القانون، ومن المتوقع أن تكون العقوبة في القانون الجديد – المزمع إصداره – قد تصل إلى الإعدام لكل من روج أو حرض على اختراق المواقع الإلكترونية الرسمية، كما يتضمن التشريع الجديد النص على غرامة مالية لكل من استولى على بريد إلكتروني خاص بأحد الأفراد، كما خول القانون الجديد لجهات الضبط حجب روابط ومحتويات المواقع التي تمارس بث صور أو عبارات أو أفلام أو أي مواد دعائية تعمل على تهديد الأمن القومي، وسواء كان ذلك البث من داخل أو خارج مصر، كما يعاقب بالسجن المشدد، كل من استخدم موقعًا على شبكة الإنترنت بقصد إنشاء وتأسيس كيان إرهابي لترويج أفكاره، أو بغرض ارتكاب أعمال إرهابية، أو بهدف تبادل الرسائل والتكليفات ونقلها بين أفراد الجماعات الإرهابية، أو تلقي أموال أو أسلحة، كما يجوز للجهات الأمنية – وفقًا للقانون الجديد – التحفظ على الأشخاص الذين يخالفون أحكام القانون، وكذا التحفظ على كافة المعدات والأجهزة المستخدمة لتحقيق ذلك، مع سرعة إيقاف خدمات البث عن أي مستخدم للإنترنت ليس له بيانات مسجلة لدى مقدم الخدمة، ويعمل مشروع القانون الجديد على مساعدة جميع المعنيين بالجرائم الإلكترونية على أداء دورهم بشكل أكثر فاعلية وقدرة على مواجهة الإرهاب الإلكتروني بكافة صوره وأنماطه.

وفي إطار الجهود المبذولة من قِبل الحكومة المصرية للتصدي للجرائم الإلكترونية، فقد تم مؤخراً رصد نحو ثلاثمائة موقعٍ إلكترونيٍ في الداخل والخارج تقوم بالتحريض على الإرهاب والعنف، كما وثّقت وزارة الداخلية نحو ثمانين بلاغًا بصفة يومية، حول العديد من الأعمال الإلكترونية التي تمس أمن وسلامة البلاد، وهو ما يرى معه البعض أن مخاطر جرائم الإنترنت، تتمثل في مدى تداول المعلومات والبيانات الخاصة، بزعزعة استقرار الأمن العام للبلاد والدعوة إلى القيام بأعمال العنف من خلال مواقع التواصل الاجتماعي، مستهدفين بذلك مؤسسات وهيئات الدولة، بالإضافة إلى تأثير الإرهاب الإلكتروني على طائفة كبيرة من جمهور المتعاطفين مع المجرمين[١].

ثانيًا– اختراق المواقع الإلكترونية في الأنظمة السعودية: في المملكة العربية السعودية جرى العمل على إصدار عدة أنظمة تهدف إلى ضبط التعاملات الإلكترونية، وتجريم العدوان أو الاعتداء

---

(١) مصر تطرح قانون "الإرهاب الإلكتروني" للنقاش والعقوبات تصل إلى الإعدام، مقال منشور على موقع صحيفة الشرق الأوسط الإلكتروني بتاريخ الأربعاء، ٢٨ ذو الحجة ١٤٣٨ هـ الموافق ٢٠ سبتمبر ٢٠١٧م، العدد رقم (١٤١٧٦)، متاح عبر الرابط:
https://aawsat.com.

الإلكتروني، ومن هذه الأنظمة نظام مكافحة الجرائم المعلوماتية[١]؛ فقد أصدرت حكومة المملكة العربية السعودية هذا النظام، والذي يهدف إلى تحقيق الأمن المعلوماتي، ومكافحة الجرائم المستحدثة، ومن هذه الجرائم المستحدثة، جرائم الحاسب الآلي وشبكات المعلومات التي تستخدم التقنية الرقمية الإلكترونية، وغيرها من الجرائم التي حرمها المنظم السعودي في المواد من (٥-٨) من هذا النظام[٢].

كما نص النظام في مادته رقم (٧) على اعتبار الدخول المتعمد إلى أنظمة الحاسب الآلي بدون وجه حقٍ جناية، تمثل اعتداءً على إجراءات الأمن، كما نصت المادة ذاتها على السجن مدة لا تزيد على عشر سنوات، وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين لكل من ينشئ موقعًا على الإنترنت لمنظمات إرهابية، أو أحد الأجهزة الإلكترونية أو نشره لتسهيل الاتصال بقيادات هذه المنظمات الإرهابية، وذلك وفق الأنظمة المرعية وحسب ما تحدده اللائحة التنفيذية[٣].

وإن من أهم صور الإجرام الإلكتروني طبقًا لهذا النظام، هي استخدام الوصفات الجاهزة لصناعة المفرقعات والقنابل مع إمكانية الحصول عليها بسهولة ويسر، ومهاجمة نظام التحكم الوطني في السكك الحديدية لإحداث تصادم بين القطارات، وفي المطارات لإحداث تصادم بين الطائرات، وتعطيل البنوك، وأعمال التحويلات المالية التي تهدف إلى تدمير الاقتصاد الوطني، وتغيير ضغط الغاز لتفجير أنابيب الغاز، وتعطيل أنظمة السلامة والأمان في المصانع الكيماوية لتفجيرها وتدميرها، وإلحاق الضرر بمن فيها، وبالبيئة المحيطة بها، والتحكم الإلكتروني عن بُعد في الأنظمة العلاجية في المستشفيات لقتل المرضى، وفي مصانع ألبان وأغذية الأطفال لتغيير وتبديل نسب المواد الغذائية بهدف قتل الأطفال، والترويع الإلكتروني وتجنيد الموالين لتنفيذ عمليات الاختراق الإلكترونية[٤].

ويرى بعض الباحثين السعوديين، أن أهم إجراءات مكافحة جريمة اختراق المواقع الإلكترونية في المملكة، تتمثل في التقنيات والتكتيكات والاستراتيجية التي تتبناها الحكومة السعودية، والإدارات الأمنية والمؤسسات الصناعية؛ وذلك لردع ومنع ورد هجمات وتهديدات الاختراق الإلكتروني، ومن أهم الوسائل الناجحة لمكافحة الجرائم الإلكترونية، ضرورة إنشاء أنظمة إنذار مبكر لصد هجمات اختراق المواقع الإلكترونية، والتطوير الدائم والمستمر لأنظمة أمن المعلومات، ونشر الوعي بخطورة وأضرار

---

(١) نظام مكافحة الجرائم المعلوماتية صدر بالمرسوم الملكي رقم: م/١٧ وتاريخ:١٤٢٨/٣/٨هـ، وهو ساري.

(٢) مصطفى محمد موسى، الإرهاب الإلكتروني، مرجع سابق، ص١١٢.

(٣) المرجع السابق، ص١١٢.

(٤) عبد العزيز بن حميدان الثمالي، تأثير الإرهاب الإلكتروني وسبل مكافحته، ضمن بحوث المؤتمر الإسلامي العالمي، والذي جاء بعنوان: الإسلام ومحاربة الإرهاب، وقد نظمته رابطة العالم الإسلامي، تحت رعاية جلالة الملك سلمان بن عبد العزيز خادم الحرمين الشريفين، وذلك في الفترة من ٣-٦ جمادى الأولى ١٤٣٦هـ/ الموافق للفترة من ٢٢- ٢٥ فبراير ٢٠١٥م والمنعقد بمكة المكرمة.

الجرائم الإلكترونية، وتطوير القدرة لدى المنظمات والحكومات والشركات على التصدي لها، مع إنشاء الإدارات المتخصصة لمكافحة هذا النوع من الجرائم[١].

ونرى: أن النظام السعودي قريب إلى حد ما من نظيره الإماراتي، في تبنيه لمنهج التطوير والتغيير المستمر والتعديل الدائم لقوانين مكافحة الجرائم الإلكترونية؛ وذلك حتى تتناسب مع طبيعة هذه الجرائم وتطورها، وخصوصاً أن بلاد الحرمين الشريفين من قائمة البلاد التي طالتها الجرائم الإلكترونية، فكانت حريصة على تعديل أنظمتها وتحديثها لتكون أشد ضراوة وأكثر ردعاً.

رابعًا – اختراق المواقع الإلكترونية في القوانين البحرينية: أصدرت المملكة البحرينية المرسوم بقانون رقم ٢٨ لسنة ٢٠٠٢ م، فيما يتعلق بالمعاملات الإلكترونية[٢]، والذي تم تعديله بموجب القانون رقم ١٣ لسنة ٢٠٠٦م.

خامسًا – اختراق المواقع الإلكترونية في القوانين اليمنية: سن المشرع اليمني فيما يتعلق بأنظمة الدفع والعمليات المالية والمصرفية الإلكترونية القانون رقم (٤٠) لسنة ٢٠٠٦م.

الفرع الثاني: اختراق المواقع الإلكترونية الرسمية في التشريعات الأجنبية

في إطار مكافحة اختراق المواقع الإلكترونية على الصعيد الدولي، ومع مسايرة التطورات الهائلة في نظم وتقنية المعلومات، فقد سنت التشريعات الأجنبية المقارنة العديد من القوانين لضبط وسلامة التعاملات الإلكترونية، وقد تضمنت هذه القوانين العديد من الجزاءات التي توقع على المخالفين في نظم التعاملات الإلكترونية، ومن هذه التشريعات التي تصدت لظاهرة الجرائم الإلكترونية: التشريع الأمريكي والفرنسي، والبريطاني، والماليزي، والكندي والإيرلندي، والنرويجي والسويسري، والسويدي، وفيما يلي إشارة موجزة عن هذه التشريعات:

أولًا – اختراق المواقع الإلكترونية في التشريع السويدي: تعد دولة السويد هي الأولى في وضع القوانين الخاصة بجرائم الإنترنت على وجه العموم، واختراق المواقع الإلكترونية بوجه خاص، فقد أصدرت السويد قانون البيانات السويدي، وكان ذلك في مرحلة مبكرة عام ١٩٧٣م؛ حيث تصدى هذا القانون لقضايا الاحتيال والنصب بواسطة الحاسب الآلي، فضلًا عن تضمنه للعديد من الفقرات العامة التي تجرم الدخول بدون وجه حق إلى بيانات الحاسب الآلي، بقصد تزويرها أو محوها أو تحويلها أو محاولة الحصول عليها بطريق غير مشروع[٣].

---

(١) المرجع السابق.

(٢) صدر في قصر الرفاع: بتاريـــخ ٧ رجب ١٤٢٣هـــ الموافق ١٤ سبتمبر ٢٠٠٢م.

(٣) عبد الرحمن عبد العزيز الشنيفي، أمن المعلومات وجرائم الحاسب الالي، ط١، الرياض، ١٤١٤هـــ، ص١٠٨.

ثانيًا – اختراق المواقع الإلكترونية في تشريعات الولايات المتحدة الأمريكية: وتلت السويد – في هذا الأمر – الولايات المتحدة الأمريكية، عندما وضعت قانونًا يتعلق بحماية أنظمة وبيانات الحاسب الآلي عام ١٩٧٦م حتى عام ١٩٨٥م، وقد بين معهد العدالة القومي عام ١٩٨٥م، خمسة أنواع تعد هي الرئيسية من أنواع الجرائم المعلوماتية، وهي تتمثل في جرائم الاستخدام غير المشروع للحاسب الآلي عن بعد، والجرائم الداخلية للحاسب الآلي، وجرائم التلاعب بالبيانات والمعلومات، وجرائم سرقة المكونات المادية والبرامج المعدة مسبقًا للحاسب الآلي، إلى أن صدر عام ١٩٨٦م قانون آخر قام فيه المشرع الأمريكي بتعريف كافة المصطلحات اللازمة؛ حتى يتسنى تطبيق القانون على الجرائم المعلوماتية، مع وضع االلتزامات الدستورية التي يتحتم مراعاتها لتطبيق القانون، وعلى ذلك فقد قامت الولايات الداخلية بإصدار القوانين الخاصة بها لبيان التعامل مع هذه الجرائم، ومن هذه الولايات: ولاية تكساس؛ حيث سنت تشريعًا لمكافحة جرائم اختراق المواقع الإلكترونية، وفي عام ٢٠٠٠م فوضت وزراة العدل الأمريكية الأمر لخمس من الجهات، في مقدمتها: مكتب التحقيقات الفيدرالي (FBI)؛ بقصد التعامل مع جرائم الإنترنت، ومنها: اختراق المواقع الإلكترونية(١).

وفي الفترة التي تولى فيها"بيل كلينتون" الرئاسة، أجرت الإدارة الأمريكية عدة خطوات تنفيذية تهدف إلى مكافحة جريمة الجرائم الإلكترونية (Cyber terrorism)؛ وتطبيقًا لذلك تم إنشاء لجنة، أطلق عليها لجنة حماية البنية الحساسة(President'sCommission on Critical Infrastructure Protectio)، ويرمز لها اختصارًا بالرمز (PCCIP)(٢)، وفي التصدي لمتاهة ضوء القمر(٣)، وتدريب نجم القمة(٤)، فقد بدأ البنتاجون حملة واسعة، والتي يهدف من وراءها التحري عن أخطر

---

(١) ممدوح عبد الحميد عبد المطلب، جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية الجريمة عبر الإنترنت، مكتبة دار الحقوق، الشارقة، ٢٠٠١م، ص٩٥.

(2) *www.fas.org/sgp/crs/homesec/RL30153.pdf*

(٣) متاهة ضوء القمر، أو (Moonlight Maze)، هي هجمة تجسس إلكتروني شنتها روسيا، على الولايات المتحدة الأمريكية، وفقًا لما ذكرته صحيفة نيويورك تايمز الأمريكية؛ حيث ذكرت أنه في السابع من أكتوبر لعام ١٩٩٦م، قامت روسيا بحادثة متاهة ضوء القمر، عندما استهدفت جهاز كومبيوتر تابع لمدرسة في ولاية (كولورادو) الأمريكية تملك عقدًا رئيسيًا مع البحرية الأمريكية. [متاح عبر الرابط الإلكتروني: http://www.roayahnews.com تمت زيارة الموقع يوم الخميس الموافق ٢٠٢١/١/٢١م في تمام الساعة الواحدة ظهرًا].

(٤) هو أيضًا تدريب روسي ضد الولايات المتحدة الأمريكية، وكان الغرض منه إجراء التجارب والتطبيقات العملية عن الدروس المستفادة من التدريب؛ حيث قام لصوص الإنترنت بالهجوم على أنظمة القوى، التي يعتمد عليها عددًا كبيرًا من القواعد العسكرية الأمريكية؛ وقاموا بزعزعة أنظمة الطوارئ في محطات الطاقة لهذه القواعد. رائد العدوان، المعالجة الدولية لقضايا الإرهاب الإلكتروني، دورة تدريبية بعنوان: توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب، في الفترة من ١٣ – ١٧/ ٤/ ١٤٣٤هـ الموافق ٢٣ – ٢٠١٣/٢/٢٧م، الرياض – المملكة العربية السعودية، ص١١].

وأشد وأعنف هجمات اختراق المواقع الإلكترونية على أنظمة الكمبيوتر الأمريكية، وذلك في مارس ١٩٩٨م [١].

ولا تتميز الولايات المتحدة الأمريكية، بأفضلية السبق في سن القوانيين المجرمة لجرائم اختراق المواقع الإلكترونية فحسب، بل تميز المشرع الأمريكي بوضع القوانين الخاصة بجميع جرائم الإنترنت، وكذلك تلك المتعلقة بتقنية المعلومات، في كافة القطاعات ذات الصلة بالاتصالات والحوسبة والإنترنت، سواء كان ذلك بشكل مباشر أو غير مباشر، وهي في الوقت نفسه تشريعات تتطور تبعًا لتطور قطاعات التقنية ذاتها، مع الاحتفاظ بكافة خصائصها المميزة لها، كما تنفرد الولايات المتحدة الأمريكية بسن عدة قوانين على المستوى الفيدرالي، فضلًا عن العديد من التشريعات على مستوى الولايات، فإن نشاط لجنة الكونجرس الأمريكي، والتي لها الولاية على حماية استخدامات الحواسيب، قد قامت بتقديم مشروع قانون حماية الحاسوب، وكان ذلك فترة سنوية مبكرة وبالتحديد عام ١٩٨٤م، بيد أن هذا القانون عدلت أحكامه بشكل جوهري حال عرضه ودراسته من لجنة الكونجرس، وبعد أن جرت عليه العديد من التعديلات والإضافات لم يتم إصداره بالاسم المشار إليه، فصدر باسم قانون غش وإساءة استخدام الحاسوب عام ١٩٨٤م، أو قانون الاحتيال وإساءة استخدام الحاسوب، وقد أضيف إلى هذا القانون، مدونة القانون الأمريكي التابعة لقسم الجرائم[٢].

ثالثًا – اختراق المواقع الإلكترونية في التشريع البريطاني: وتأتي بريطانيا في المرتبة الثالثة بعد السويد والولايات المتحدة الأمريكية؛ من حيث سن القوانين الخاصة بجرائم اختراق المواقع الإلكترونية، فأقرت قانون مكافحة التزوير والتزييف عام ١٩٨١م، والذي يتضمن التعرض لبيان أدوات التزوير ووسائط التخزين المختلفة، أو أي أداة من الأدوات الأخرى التي تستخدم للتسجيل عليها بطريقة تقليدية أو إلكترونية أو أي طريقة أخرى[٣].

وكذلك قانون إساءة استخدام الحاسوب (Computer Misuse Act)، وهو القانون الذي وضعته الحكومة البريطانية عام ١٩٩٠م، وبدأ العمل به في ١٩٩٠/٨/٢٩م، وقد تبنى هذا القانون بعض الجرائم الجديدة والتصدي لها، وتتمثل هذه الجرائم في الدخول غير المشروع إلى البيانات بقصد العبث أو التطفل، أو بهدف ارتكاب أو تسهيل ارتكاب أفعال أخرى، أو تعديلها أو تحويرها، أو إضعاف أو تعطيل النظام.

---

(١) رائد العدوان، المعالجة الدولية لقضايا الإرهاب الإلكتروني، مرجع سابق، ص١١.

(٢) عادل عبد الصادق، الفضاء الإلكتروني والعلاقات الدولية – دراسة في النظرية والتطبيق، المكتبة الأكاديمية، القاهرة، ٢٠١٦م، ص٢١٣.

(٣) عبد الرحمن عبد العزيز الشنيفي، أمن المعلومات وجرائم الحاسب الالي، مرجع سابق، ص١٠٩.

رابعًا – اختراق المواقع الإلكترونية في التشريع الفرنسي: بينما كان مجلس الشيوخ الفرنسى ينظر مشروع قانون أعد لتعديل قانون حرية الاتصالات الصادر عام ١٩٨٦م ليتفق مع التوجهات الأوربية الجديدة تقدمت الحكومة الفرنسية بتعديل لهذا المشروع سمى بقانون فيون FILLON وزير الاتصالات الفرنسى فى ذلك الوقت، وانطوى هذا التعديل على إضافة مواد جديدة للقانون الصادر فى ٣٠ سبتمبر ١٩٨٦م بشأن الإذاعة والتليفزيون، واستهدفت الحكومة من هذا التعديل تعريف القائم على تقديم خدمة الإنترنت(١).

كما جرم المشرع الفرنسي مجرد الدخول إلى أنظمة المعالجة الآلية أو البقاء بدون تصريح، وذلك وفقًا لما ورد النص عليه في القانون رقم (١٩–٨٨) والصادر في الخامس من كانون الثاني عام ١٩٨٨م بشأن بعض الجرائم المعلوماتية، والذي تضمنه المشرع في المادة (٤٦٢) بفقرتيها: الأولى والثانية من قانون العقوبات الفرنسي، وقد شدد المشرع الفرنسي في هذا القانون – الذي أدخل عليه تعديلات عام ١٩٩٣م – العقوبات في الحالات التي يترتب على الدخول غير المشروع محو أو تعديل في المعطيات أو البيانات التي تم معالجتها آليًا، أو تزوير المستندات واستعمالها في غير الغرض المخصص لها، وكانت العقوبة تتراوح ما بين الحبس أو الغرامة(٢) .

وبخصوص الرقابة الإدارية على وسائل الاتصالات الخاصة، والتي تسمى بالمراقبة الأمنية Interceptions de sécurité فإن المشرع الفرنسي حدد حالاتها على سبيل الحصر؛ وذلك في بالمادة الثالثة من قانون العاشر من يوليو لعام ١٩٩١م بشأن سرية المراسلات، فإنه لا تجوز المراقبة إلا للبحث عن معلومات تتعلق بالأمن القومى والمحافظة على المركز العلمى والاقتصادى لفرنسا، ولمكافحة اختراق المواقع الإلكترونية وإعادة تنظيم الجماعات التى تم حلها بمقتضى قانون عام ١٩٣٦م بشأن جماعات القتال والفرق الخاصة، ويتعين إعدام متعلقات التسجيلات والمراقبة بانتهاء الغرض منها، ولقد أنشأ قانون١٩٩١م لجنة تسمى اللجنة القومية لمراقبة التسجيلات الأمنية (Commission nationale de contrôle des interceptions de sécurité)(٣).

خامسًا – اختراق المواقع الإلكترونية في التشريع النرويجي: في عام ١٩٨٥م أجرى المشرع النرويجي تعديلًا على قانون العقوبات، وقصد من ورائه تجريم الوصول غير المشروع بواسطة تخطي

---

(١) مدحت رمضان، جرائم الانترنت، في الدورة المنعقدة بمركز الأستاذ الدكتور/عبد الرءوف مهدى للبحوث الجنائية بكلية الحقوق جامعة المنصورة، يوم السبت الموافق ٢٠١٢/٣/١٧م، ص٩.

(٢) أحمد حسام طه تمام: الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، ٢٠٠٠م، ص٢٢٢.

(3) Le Comité supérieur de la télématique

الحماية، إلى المعلومات أو البيانات السابق تخزينها، أو التي تم نقلها بوسيلة إلكترونية أو فنية أخرى، ومن ثم عقاب من أتلف أو عطل هذه البيانات، أو استخدمها بطريقة غير مشروعة[١].

سادسًا – اختراق المواقع الإلكترونية في التشريع السويسري: من جانبه فإن قانون الجرائم المعلوماتية السويسري لعام ٢٠١٣م، قد اشتمل في مواده النص على عقاب من يحصل على البيانات المخزنة إلكترونيًا بطريق غير مشروع، وكذلك عقاب من يحصل على البرامج بهدف الحصول على المال على نحو غير مصرح به، أو محاولة الوصول إلى أنظمة الحاسوب وإتلاف محتوياتها أو محو بياناتها[٢].

سابعًا– اختراق المواقع الإلكترونية في التشريع الكندي: تطبق كندا القوانين الأكثر تخصصًا وتفصيلًا للتعامل مع جرائم الإنترنت؛ فقد عاقب المشرع الكندي، فإن جميع من أوقف أو اعترض، بأي وسيلة، سواء بالغش أو بدون وجه حق، أو أنه كان سببًا في عرقلة أي من وظائف الحاسوب، كما جرم من يحصل بغش على خدمة مقدمة من الحاسب، أو على استخدام أو التسبب في استخدام الحاسب ليرتكب أي من الجرائم، كما عاقب المشرع كل من أتلف البيانات، وكان ذلك وفقًا لنص المادة (٢/٣٠١) في التعديل الذي أجراه المشرع الكندي على قانون العقوبات عام ١٩٨٥م، بحيث ضمنه في هذا التعديل بعض جرائم الحاسب الآلي والإنترنت، كما تضمن بيان العقوبات لمن يرتكب مخالفة من المخالفات الحاسوبية، كما تضمن جرائم التمييز والدخول غير المصرح به لنظام الحاسب، ولم يخلُ القانون الجنائي الكندي من بيان صلاحيات جهات التحقيق، وهو ما ورد في قانون المنافسة الذي يخول لمأمور الضبط القضائي – حال حصوله على أمر قضائي – حق تفتيش وفحص الحواسيب الآلية وضبطها[٣].

ثامنًا – اختراق المواقع الإلكترونية في التشريع الدنماركي: ومن جهتها فقد سنت الدنمارك عام ١٩٨٥م بكورة قوانينها فيما يتعلق بجرائم الحاسب الآلي الإنترنت، وقد تضمن القانون العقوبات المحددة لمرتكب جرائم الحاسب الآلي، كجريمة التزوير أو الدخول غير المشروع إلى أنظمة الحاسب الآلي أو اختراق المواقع الإلكترونية، أو الكسب بطريق غير مشروع، سواء كان ذلك للجاني أو لطرف

---

(١) عادل عبد الصادق، الفضاء الإلكتروني والعلاقات الدولية – دراسة في النظرية والتطبيق، المكتبة الأكاديمية، مرجع سابق، ص٢٢٦.

(2) HUET JEROME et MAISL HERBERT, DROIT DE L'INFORMATIQUE ET DES TELECOMMUNICATIONS, DROIT PRIVE ...DROIT PUBLIC, LITEC, 1989, p.868, no. 726.

(٣) أحمد هلالي عبد اللاه، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي – دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٦م، ص٢٦٣.

آخر أو التلاعب غير المشروع ببيانات الحاسب الآلي؛ كالقيام بإتلافها أو تغييرها أو الاستفادة منها بأي وجه من الوجوه[١].

تاسعًا – اختراق المواقع الإلكترونية في التشريع الفنلندي: في عامي ١٩٩٠م، ١٩٩٥م، أدخل المشرع الفنلندي تعديلات على قانون العقوبات؛ بناء على الاقتراح المقدم من اللجنة المكلفة بدراسة جرائم الإنترنت، وقد تضمنت التعديلات تجريم كافة صور الوصول غير المشروع إلى أنظمة البيانات، وذلك بمحاولة فك كلمة السر أو كسر الرقابة التأمينية؛ ومن ثم استخدام الكمبيوتر في ارتكاب جريمة الاحتيال أو التزوير[٢].

عاشرًا – اختراق المواقع الإلكترونية في التشريع الأيرلندي: ومن جانبها وفي عام ٢٠٠١م، أصدرت إيرلندا نظاماً يهدف إلى حماية الأفراد من الجرائم المعلوماتية؛ حيث يتيح هذا النظام معاقبة الاستخدام غير المسموح به، أو غير المشروع للأجهزة والأنظمة المتعلقة بالحاسب الآلي[٣].

حادي عشر – اختراق المواقع الإلكترونية في التشريع الماليزي: في عام ١٩٩٧م أصدرت ماليزيا نظاماً للمخالفات الإلكترونية، وقد صنف هذا النظام المخالفات الإلكترونية إلى: الوصول غير المسموح به أو غير المشروع إلى الحاسب الآلي، والدخول إليه بنية التدمير أو التخريب أو الإزالة أو التعديل غير المصرح به؛ حيث تتراوح العقوبات المحددة لهذه الجرائم ما بين الغرامات المالية، التي قد تصل إلى مائة وخمسين ألف دولار ماليزي[٤]، إلى الحبس والسجن الذي تصل مدته إلى عشر سنوات.

الخاتمة

نخلص من هذه الدراسة إلى أهم النتائج والتوصيات الآتية:

أولًا – النتائج"

---

(١) أ. عبد الرحمن عبد العزيز الشنيفي، أمن المعلومات وجرائم الحاسب الالي، مرجع سابق، ص١١٠.

(٢) رائد العدوان، المعالجة الدولية لقضايا الإرهاب الإلكتروني، مرجع سابق، ص١٢.

(٣) عبد الله بن سعود الموسى، التحريض على الجريمة الإرهابية بين الشريعة الإسلامية والقانون الوضعي – دراسة مقارنة، رسالة ماجستير، جامعة نايف للعلوم الأمنية، الرياض، ١٤٢٧هـ/٢٠٠٦م، ص١٢٩.

(٤) محمد القاسم، رشيد الزهراني، عبد الرحمن السند، عاطف العمري: دراسة تجارب الدول في مجال أحكام في المعلوماتية، مشروع الخطة الوطنية لتقنية المعلومات، ١٤٢٣هـ.

(١) أن اختراق المواقع الرسمية للدولة: هو حالة الدخول غير المشروع إلى مواقع إلكترونية أو نظام معلوماتي بطريقة مباشرة عن طريق شبكة المعلومات الدولية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات ومعلومات ماسة بالأمن الداخلي أو الخارجي للبلاد

(٢) أنه لا يجوز المساس بمحتوي البريد الإلكتروني أو تفتيش هذا المحتوي داخل الكمبيوتر أو الإطلاع علي مكنونه أو أسراره بالتنصت أو التفتيش إلا بإذن قضائي مسبب ، وهو ما اضطرد عليه القضاء الأمريكي في العديد من الأحكام.

(٣) انفردت الجرائم الإلكترونية بخصائص وميزات ميزتها عن الجرائم التقليدية نظراً لطبيعتها التي ترتكب في بيئة غير تقليدية تقع خارج إطار الواقع المادي الملموس يطلق عليها البيئة الإلكترونية من حيث أنها تكتسب خصوصية غير عادية وهي جرائم جديدة في شكلها ووسائلها ومخاطرها بلون وثوب جديدين

(٤) أسفر الواقع المعاصر عن ان الجرائم المرتكبة على الأموال والاتصالات من اخطر الجرائم الالكترونية المستحدثه كون هذه الجرائم تؤدي للكثير من الخسائر المادية الضخمه فالجرائم التقليدية لا تتم إلا بالسطو على المؤسسات المالية او الشركات وهي بذلك تحتاج إلى تخطيط مسبق ومجهود عضلي جماعي بخلاف الجرائم المالية الالكترونية التي تتم بسهوله فكل ما تحتاجه ان يتوافر لدى الجاني الدراية الكافية ببرامج الكمبيوتر.

(٥) تعد فكرة استخدام آلة (كمبيوتر) في معالجة الأرقام ليست بالجديدة[١]؛ حيث أشار بعض الباحثين إلى استخدام مثل هذه الوسيلة – في صورتها الأولى – وجد في آسيا منذ خمسة آلاف عام[٢]، كما مهدت الثورة الصناعية، منذ منتصف القرن الماضي ومن خلال التقدم التقني في مجال الحواسيب الآلية، لبزوغ ثورة جديدة هي ثورة المعلومات، وما أدت إليه من جرائم إلكترونية.

(٦) تزايدت مخاطر الجرائم الإلكترونية في الآونة الأخيرة، وعلى وجه التحديد منذ بزوغ فجر الثورة التكنولوجية وما أفرزته من آثار سلبية نجم عنها ظهور جريمة جديدة غير معروفة؛ ألا وهي جريمة اختراق المواقع الإلكترونية؛ حيث يعد هذا النوع من الجرائم، أشد خطراً وأعظم ضرراً من الجرائم التقليدية، وعلى وجه الخصوص في مستواها الفني والتقني التي يتميز بها المجرم الإلكتروني.

(٧) أن التزايد في معدل الحوادث الإلكترونية ما هو إلا بسبب دخول الإنترنت، وعلى وجه الخصوص اختراق المواقع الإلكترونية، وغير ذلك من الجرائم غير العمدية والتي تزايدت زيادة مضطردة.

ثانيًا – التوصيات:

---

(١) سعيد عبد اللطيف حسن: إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، ط١، بدون دار طبع، ١٩٩٩م، ص١٣.

(2) Walsh (John) , Standard Grade – Computing Studies – 1994. pp. 308. Bill Gates , The Road Ahead 1995 p. 93 – 99.

(١) نوصي المشرع بضرورة تغليظ العقوبات المقررة لجريمة اختراق المواقع الرسمية، وذلك لتعلقها بالصالح العم، وتتضمنها أسرار الدولة.

(٢) نوصي المشرع بضرورة سن تشريع خاص بهذه الجريمة.

(٣) نوصي المشرع ببيان مفهوم هذه الجريمة على وجه الدقة، وما يعد اختراقًا مما لا يعد كذلك، وذلك حتى لا تختلط بعيرها من الجرائم الإلكترونية.

قائمة المصادر والمراجع

أولًا – المراجع العربية:

- أحمد أسامة حسنية، الجريمة الإلكترونية بين الشرعية الجنائية والإجرائية، مجلة جامعة الأزهر، غزة، عدد خاص بمؤتمر كلية الحقوق الخامس، المحكم، المجلد ١٩، ٢٠١٧م.
- أحمد أسامة حسنية، الجريمة الإلكترونية بين الشرعية الجنائية والإجرائية، مرجع سابق، ص٦؛
- أحمد حسام طه تمام: الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، ٢٠٠٠م.
- أحمد خليفة الملط، الجرائم المعلوماتية، ط٢، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م، أسامة أحمد المناعسة، وجلال محمد الزعبي، جرائم تقنية نظم المعلومات الالكترونية – دراسة مقارنة، ط٣، دار الثقافة للنشر وتوزيع، عمان – الأردن، ٢٠١٧م
- أحمد هلالي عبد اللاه، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي – دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٦م.
- أيمن عبد الله فكري، جرائم أنظمة المعلومات، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٧م
- بحوث مؤتمر القانون والكمبيوتر والإنترنت، المجلد الثاني، ط٣، جامعة الإمارات العربية المتحدة، ٢٠٠٤
- بهاء المري، شرح قانون مكافحة جرائم تقنية المعلومات وحجية الدليل الرقمي في الإثبات، العربية للنشر والتوزيع، القاهره، ٢٠١٩م
- حسن طاهر داوود، جرائم نظم المعلومات، ط١، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٠م، ص٢٠٩؛ محمد الأمين البشري، بحث بعنوان: التحقيق في جرائم الحاسب الآلي، مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، الذي تم انعقاده في كلية الشريعة والقانون بدولة الإمارات العربية المتحدة، في الفترة من الأول إلى الثالث من شهر مايو لعام ٢٠٠٠م.

- حسين بن سعيد الغافري، السياسة الجنائية في مواجهة الإنترنت – دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٩م
- رائد العدوان، المعالجة الدولية لقضايا الإرهاب الإلكتروني، دورة تدريبية بعنوان: توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب، في الفترة من ١٣ – ١٧/ ٤/ ١٤٣٤هـ الموافق ٢٣ – ٢٠١٣/٢/٢٧م، الرياض – المملكة العربية السعودية.
- سعيد عبد اللطيف حسن: إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، ط١، بدون دار طبع، ١٩٩٩م
- صدر هذا القانون في قصر الرئاسة بمدينة أبو ظبي، بتاريخ ٣٠ ذي الحجة ١٤٢٦هـ، الموافق ٣٠ يناير ٢٠٠٦م.
- عادل عبد الصادق، الفضاء الإلكتروني والعلاقات الدولية – دراسة في النظرية والتطبيق، المكتبة الأكاديمية، القاهرة، ٢٠١٦م
- عبد الاله النوايسة، جرائم تكنولوجيا المعلومات – شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، ط١، دار وائل للنشر والتوزيع، عمان – الأردن، ٢٠١٧م
- عبد الحميد إبراهيم محمد العريان، العلاقة بين الإرهاب المعلوماتي والجرائم المنظمة: ما هو رد فعل القطاع الخاص، بحث ضمن دورة تدريبية بعنوان: مكافحة الجرائم الإرهابية المعلوماتية، خلال الفترة من: ١١–١٤٢٧/٣/١٥هـ، الموافق ٩– ٢٠٠٦/٤/١٣م، المغرب – القنيطر
- عبد الرحمن عبد العزيز الشنيفي، أمن المعلومات وجرائم الحاسب الالي، ط١، الرياض، ١٤١٤هـ
- عبد العزيز بن حميدان الثمالي، تأثير الإرهاب الإلكتروني وسبل مكافحته، ضمن بحوث المؤتمر الإسلامي العالمي، والذي جاء بعنوان: الإسلام ومحاربة الإرهاب، وقد نظمته رابطة العالم الإسلامي، تحت رعاية جلالة الملك سلمان بن عبد العزيز خادم الحرمين الشريفين، وذلك في الفترة من ٣–٦ جمادى الأولى ١٤٣٦ه/ الموافق للفترة من ٢٢– ٢٥ فبراير ٢٠١٥م والمنعقد بمكة المكرمة.
- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دار الكتب القانونية، المحلة الكبرى، مصر، ٢٠٠٦م

- عبد الله بن سعود الموسى، التحريض على الجريمة الإرهابية بين الشريعة الإسلامية والقانون الوضعي – دراسة مقارنة، رسالة ماجستير، جامعة نايف للعلوم الأمنية، الرياض، ١٤٢٧هـ/٢٠٠٦م
- عبد الله حسين محمود، إجراءات جمع الأدلة في مجال سرقة المعلومات، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات المنعقد في الفترة ٢٦–٢٨ أبريل ٢٠٠٣م، دبي – الإمارات العربية المتحدة
- عبد الله علي عبد الله القحطاني، إدارة أمن المعلومات ودورها في الحد من الإرهاب الإلكتروني بكلية الحسابات وتقنية المعلومات بجامعة الملك عبد العزيز بجدة، رسالة ماجستير، جامعة نايف للعلوم الأمنية، الرياض – المملكة العربية السعودية، ١٤٣٨هـ/٢٠١٧م
- عبد المجيد الحلاوي، أهمية التعاون العربي والدولي في محكافحة جرائم الإرهاب المعلوماتي، بحث ضمن دورة تدريبية بعنوان: مكافحة الجرائم الإرهابية المعلوماتية، خلال الفترة من: ١١–١٤٢٧/٣/١٥هـ، الموافق ٩– ٢٠٠٦/٤/١٣م، المغرب – القنيطرة.
- عبيد صالح حسن، سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية، مجلة الفكر الشرطي، المجلد رقم (٢٤) – العدد رقم (٩٥) أكتوبر، ٢٠١٥م
- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديدة للنشر، الإسكندرية، ١٩٩٧م
- علي عبد القادر القهوجي، الحماية الجنائية لجرائم الحاسب، بحث منشور بمجلة الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية، العدد ٢٤، ١٩٩٢م
- لورنس حوامدة، الجرائم المعلوماتية وأركانها وآلية مكافحتها – دراسة تحليلية مقارنة، بحث منشور في مجلة الميزان للدراسات الإسلامية والقانونية، جامعة العلوم الإسلامية، المجلد الرابع، العدد الأول، كانون الثاني، ٢٠١٧م
- محمد إبراهيم محمد الشافعي، النقود الإلكترونية، مجلة الأمن والحياة، أكادمية شرطة دبي، يناير٢٠٠٤م
- محمد أحمد محمد الحمادي، تشريعات مكافحة جرائم تقنية المعلومات في دولة الإمارات وأحكام القضاء، دولة الإمارات العربية المتحدة، أبوظبي، شرطة أبوظبي، مركز الدراسات الأمنية، ورقة عمل قدمها الباحث في ندوة شبكات الإنترنت وتأثيراتها الاجتماعية والأمنية، ط٢، في الفترة من (٦–٧) من شهر نوفمبر لعام ٢٠٠٦م

- محمد الأمين الشوابكه، جرائم الحاسوب والانترنت الجريمة المعلوماتية، مرجع سابق، ص١٢٠.
- محمد القاسم، رشيد الزهراني، عبد الرحمن السند، عاطف العمري: دراسة تجارب الدول في مجال أحكام في المعلوماتية، مشروع الخطة الوطنية لتقنية المعلومات، ١٤٢٣هـ.
- محمد أمين الشوابكة، جرائم الحاسوب والإنترنت الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان – الأردن، ٢٠١٥م
- محمد حماد مرهج الهيتي، جرائم الحاسوب – دراسه تحليلية، ط١، دار المناهج، عمان – الأردن، ٢٠٠٦م
- محمد سامي الشوا: ثورة المعلومات وانعكاساتها علي قانون العقوبات، دار النهضة العربية، القاهرة، ٢٠٠٣م
- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، ط٢، دار النهضة العربية، القاهرة، ١٩٩٨م
- محمد سيد محمد، وسائل الإعلام من المنادي إلى الإنترنت، دار الفكر العربي، القاهرة، ٢٠٠٩م
- محمد عبد الرحيم سلطان، جرائم الإنترنت والاحتساب عليها، مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات، العين، مايو ٢٠٠٠م
- محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٤
- محمود عبد العزيز أبو زيد، الحماية الجنائية لتكنولوجيا الحاسب الآلي والنظم المعلوماتية، رسالة دكتوراه، كلية الحقوق – جامعة القاهرة، ٢٠١٦م
- محمود مدين، الجريمة الإلكترونية وتحديات الأمن القومي، المصرية للنشر والتوزيع، القاهرة، ٢٠١٩م
- محمود نجيب حسني، شرح قانون العقوبات القسم العام، دار النهضه العربية، القاهره، ٢٠١٦م.
- مدحت رمضان: جرائم الانترنت، في الدورة المنعقدة بمركز الأستاذ الدكتور/عبد الرءوف مهدى للبحوث الجنائية بكلية الحقوق جامعة المنصورة، يوم السبت الموافق ٢٠١٢/٣/١٧م
- مصطفى محمد موسى: الإرهاب الإلكتروني، دراسة (قانونية – أمنية – نفسية – اجتماعية) ط١، سلسلة اللواء الأمنية في مكافحة الجرائم الإلكترونية،١٤٣٠هـ/٢٠٠٩م،

- ممدوح عبد الحميد عبد المطلب: جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية الجريمة عبر الإنترنت، مكتبة دار الحقوق، الشارقة، ٢٠٠١م
- نائل عبد الرحمن صالح، واقع جرائم الحاسوب في التشريع الأردني، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ٢٠٠٠م.
- نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، دار النهضة العربية، القاهرة، ٢٠٠٤م.
- نبيل عبد المنعم جاد، أسس التحقيق والبحث الجنائي العلمي، مطبعة كلية الشرطة، القاهرة، ٢٠٠٥م
- نبيلة هبة هروال، جرائم الإنترنت – دراسة مقارنة، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد – الجزائر، ٢٠١٣م/ ٢٠١٤م
- هدى قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، ط١، دار النهضه العربية، القاهره، ١٩٩٢م.
- هشام محمد فريد رستم، الجرائم المعلوماتية أصول التحقيق الجنائي الفني، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ٢٠٠٠م.
- هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤م نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الإسكندرية ، ٢٠٠٨مهلالي عبد اللاه أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية – دراسة مقارنة، دار النهضة العربية، القاهرة، ١٩٩٧م
- يونس عرب، جرائم الانترنت، إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الاجرائية للملاحقة والإثبات، ورقة عمل، مقدمه إلى مؤتمر الأمن العربي، ٢٠٠٢م، المنظم بالمركز العربي للدراسات والبحوث الجنائية، أبوظبي، في ٢٠١٢/١٢/١٠م.

ثانيًا – المراجع الأجنبية:

- Bouzat . J. pinatel . Traité ole droit penal et de Criminologie . Toml Droit penal , Paris .

- Bouzat. J. pinatel. Traité ole droit penal et de Criminologie. Toml Droit penal , Paris.
- Chen – christopher D. Computer Crime , The Computer Fraud and Abuse act of 1986 , C.L.J... 1990 , Vol 10 .
- Chen – christopher D. Computer Crime , The Computer Fraud and Abuse act of 1986 , C.L.J... 1990 , Vol 10.
- D.B. Parker , Combattre La Crimpinalité informatique , éd Oros : 1985.
- First Annual Cost of Cyber Crime Study, Peneman Institute, Research Report MI.2010.
- HUET JEROME et MAISL HERBERT, DROIT DE L'INFORMATIQUE ET DES TELECOMMUNICATIONS, DROIT PRIVE ...DROIT PUBLIC, LITEC, 1989.
- HUET JEROME et MAISL HERBERT, DROIT DE L'INFORMATIQUE ET DES TELECOMMUNICATIONS, DROIT PRIVE ...DROIT PUBLIC, LITEC, 1989.
- J. Devéze , Les Qualifications Penalesaux Fraudes informatiques , in Le droit Criminel Face au techniques de communication lieés à l'informatique.
- J. Devéze , Les Qualifications Penalesaux Fraudes informatiques , in Le droit Criminel Face au techniques de communication lieés à l'informatique.
- K. Tiedemnn , Fraude et autres délits d'afaires commis à l'aide d'ordinateurs électroniques ,Rev. droit penal crim. 1984 p. 612 .
- K. Tiedemnn , Fraude et autres délits d'afaires commis à l'aide d'ordinateurs électroniques ,Rev. droit penal crim. 1984 p. 612 .
- Kataz, Berger . v . New York , 388 , U . S . , 41 1967. . www.lex.electronica-org/articles,v6-21pepin.htm.

- M.Masse. la droit pénal special né del'informatique et doit pénal , Travaux de l'institut de sciences criminelles de poietiers 1981- léd cujas p. 23 .
- Michel vivant et autres , Droit de l'informatique et des réseaux , Lamy , 2001 , p. 1837 .
- Schiolberg (s) – Computers and penal Leg is Lation, as tudy of the Legal politics of a new technology ,1983, p4 .
- TORTELLO NICOLE & LOINTIER PASCAL, INTERNET POUR LES JURISTES, DALLOZ, 1996
- Walsh (John) , Standard Grade – Computing Studies – 1994. pp. 308. Bill Gates , The Road Ahead 1995