العدد الثامن والعشرون
تاريخ الإصدار: 2 – شباط – 2021 م
www.ajsp.net
ISSN: 2663-5798

"مدى كفاية الحماية الجزائية في التشريع الاردني لمواجهة جرائم الارهاب الالكتروني"

اعداد الباحث:
طايل مازن القاضي

العدد الثامن والعشرون
تاريخ الإصدار: 2 – شباط – 2021 م
www.ajsp.net
ISSN: 2663-5798

الملخص:

هدفت هذه الدراسة الى التعرف على الجرائم الالكترونية بشكل عام وجرائم الارهاب الالكتروني بشكل خاص، وموقف المشرع الجزائي الاردني من جرائم الارهاب الالكتروني ومقارنة ذلك مع بعض التشرعات المقارنة، وتناولت هذه الدراسة الجرائم الالكترونية بشكل عام وجرائم الارهاب الالكتروني بشكل خاص بمنهج وصفي تحليلي مقارن يقوم على وصف ظاهرة الجرائم الالكترونية وجرائم الارهاب الالكتروني، ومن أهم النتائج التي توصل إليها الباحث من خلال هذه الدراسة ان نظام المعلومات مصطلح واسع الدلالة يشمل في معناه المكونات المادية لأجهزة الحاسوب أو الشبكات التي تربط بينها كما يشمل البيانات والمعلومات والبرامج وقواعد البيانات والمصنفات الأخرى التي يتم إعدادها بوساطة الحاسوب، وتعد المعلومات المخزنة في جهاز الحاسوب أموالا مادية منقولة، وتوصل الباحث الى العديد من **التوصيات اهمها:** ضرورة تدخل المشرع بالنص على تجريم جريمة الإرهاب الإلكتروني من خلال نصوص خاصة على الرغم من صلاحية المعلومات من حيث المبدأ لأن تكون محلاً لجريمة الإتلاف بمقتضى النصوص التقليدية في قانون العقوبات باعتبارها أموالاً مادية منقولة

الكلمات المفتاحية: الحماية الجزائية، التشريع الأردني، جرائم الارهاب الالكتروني.

المقدمة:

أصبح الإرهاب ظاهرة خطيرة تهدد حياة الناس اليومية ، في أي مكان و زمان في أنحاء العالم، ويظهر ذلك من خلال التزايد الكبير في العمليات الإرهابية و تنوع صورها واتخاذها أشكالا متعددة وامتدادها إلى مختلف بلدان العالم رغم توجهاتها السياسية أو انتمائها الإيديولوجية، لما تمتاز به هذه الجريمة من آثار مدمرة تشمل الحضارة الإنسانية جمعاء ، حيث اتخذت هذه الجريمة العديد من الأشكال والأساليب المستحدثة والتي من الصعوبة بمكان ضبطها والسيطرة عليها.

لقد بذلت الأردن جهود كبيرة وعديدة بهدف الوصول إلى الآليات المناسبة التي تحد من العمليات الإرهابية، كخطوة رئيسية في وضع عقوبة لها تكون رادعة ومناسبة بشكل كاف، وأمام انتشار هذه الظاهرة، سعت دول العالم إلى وضع التشريعات المتنوعة، لمنع هذه الظاهرة، حيث سعت بعض الدول على العمل إلى وضع التشريعات المنفصلة عن باقي التشريعات فيها، فأصدرت قوانين لمنع ظاهرة الإرهاب و الحد منها .

ومن هذه الدول، كانت الدول العربية التي سعت إلى سن تشريعات خاصة بالإرهاب، لتكون آليات قانونية متقدمة تواكب انتشار ظاهرة الإرهاب في العالم، ومن هذا المنطلق سعى الأردن لسن الآليات القانونية لمنع حدوث الأعمال الإرهابية، وملاحقة مرتكبيها عن طريق وضع تشريعات تحدد العقوبات الرادعة لتلك الظاهرة التي أصبحت تمارس على الدوام . [1]

أهمية الدراسة:

يكتسب موضوع هذه الدراسة أهمية متزايدة بسبب استغلال وسائل الاتصال الحديثة من قبل مرتكبي الجرائم لتسهيل ارتكابهم لجرائمهم.

([1]) مثل قانون العقوبات الأردني رقم 16 الصادر عام 1960، قانون منع الإرهاب الأردني رقم (55) لسنة 2006، قانون رقم 46 لسنة 2007 الخاص بمكافحة غسل الأموال و تمويل الإرهاب و تعديلاته . انظر مشهور العريمي ، الشرعية الدولية لمكافحة الإرهاب ، دار لثقافة للنشر و التوزيع ، عمان ، 2009، ص 13

إن لموضوع هذه الدراسة أهمية نظرية وعملية لكونه يمس كثيراً من مصالح المجتمع، كما تظهر أهميته في تحديد مصادر المخاطر التي تهدد النظام الإلكتروني ونظم الشبكات، وتحديد صور الاعتداء على المعلومات، والأنماط المستجدة للجرائم الإلكترونية، كما تظهر أهمية الموضوع من خلال التعرف على الاتجاهات التشريعية الدولية والإقليمية لحماية المعلومات ونظمها الإلكترونية.

مشكلة الدراسة وأسئلتها:

إن التطور التقني لأساليب ارتكاب الجرائم وخصوصاً تلك التي تتم عبر الإنترنت والحاسوب ووسائل التواصل الاجتماعي، تتطلب اصدار قوانين جزائية تحدد اركان وعناصر الجرائم الالكترونية، حيث ان هذه الجرائم اصبحت تتمتع باركان وعناصر تميزها عن الجرائم التقليدية هذا من جهة، ومن جهة اخرى بناء الثقة والامان في استعمال تكنولوجيا المعلومات من خلال ملاحقة وعقاب الذين يسيئون استعمال تكنولوجيا المعلومات لاغراض اجرامية، لذلك تكمن مشكلة الدراسة في بيان مدى كفاية الحماية الجزائية في التشريع الاردني لمواجهة جرائم الارهاب الالكتروني.

وتتضمن هذه الدراسة الاجابة عن التساؤلات التالية

1. ماهية الجرائم الالكترونية وخصائصها؟
2. ماهية الإرهاب في التشريعات الوطنية و الإقليمية و الدولية؟
3. ما المقصود بجرائم الإرهاب الإلكتروني؟
4. ما أركان جريمة الإرهاب الإلكتروني؟

أهداف الدراسة

تهدف هذه الدراسة الى التعرف على الجرائم الالكترونية بشكل عام وجرائم الارهاب الالكتروني بشكل خاص، وموقف المشرع الجزائي الاردني من جرائم الارهاب الالكتروني ومقارنة ذلك مع بعض التشرعات المقارنة. كما تهدف الى تحقيق ما يلي:

1- بيان ماهية الجرائم الالكترونية من خلال المفهوم والخصائص وسمات مرتكبيها والاركان وتعريف الارهاب في التشريعات الوطنية والاقليمية والدولية.
2- دراسة الآثار المترتبة على جريمة الإرهاب الإلكتروني.

الدراسات السابقة:

- دراسة (Hamid, 2010) بعنوان: **"الحماية الجنائية للمعلومات الإلكترونية"**، رسالة ماجستير، جامعة عين شمس.

تناول الباحث التحول إلى التطبيقات الإلكترونية، والوقوف على النصوص التي تنظم هذه المسؤولية، ومقارنتها بالتطورات التي طرأت على أساليب ارتكاب مثل هذه الجرائم المستحدثة، وبحث مدى تناسب تطبيقها على هذه الجرائم، إضافة إلى اقتراح الحلول التشريعية لمكافحة جرائم المعلومات التي ارتبطت بالتطور التقني وما صحبه من ثورة تقنية في مجال المعلومات أو المعرفة على مستوى العالم. وتوصل الباحث إلى نتائج، منها: أن دولة الإمارات العربية المتحدة كانت من أوائل الدول التي تصدت للجرائم المعلوماتية أو الإلكترونية، وذلك من خلال إصدار القانون الاتحادي رقم (2) لسنة 2006م في شأن مكافحة جرائم تقنية المعلومات، كما تم إنشاء دوائر قضائية متخصصة للنظر في الجرائم الإلكترونية.

- دراسة (Khawaldeh, 2012) بعنوان: **"جريمة الدخول غير المشروع إلى موقع إلكتروني أو نظم معلومات وفق التشريع الأردني – دراسة مقارنة"**، دار الثقافة، عمان.

تناول الباحث الطبيعة القانونية لجريدة الدخول غير المشروع لموقع إلكتروني أو نظام معلومات وذلك بتطبيقها على واقع النص القانوني من خلال وصف أركان هذه الجريمة وصور النشاط الجرمي المكون لها، ومسؤولية مرتكب هذا النوع من الجرائم المستحدثة، والجزاء المقرر لها وفق نصوص قانون جرائم أنظمة المعلومات الأردني لعام 2010م مقارنة مع بعض التشريعات الجنائية المقارنة، وخلصت الدراسة إلى عدد من النتائج والتوصيات، كان من أهمها: أنه من الضروري إدخال نصوص قانونية تعاقب على جريمة إتلاف المعلومات والبيانات بحد ذاتها وتقرر مسؤولية الشخص المعنوي في حال ارتكاب الجرائم المعلوماتية، والمعاقبة على الشروع في مثل هذه الجرائم.

حدود الدراسة:

الحدود المكانية:

اقتصرت بصفة أساسية على التشريع الأردني، مع التعرض لبعض التشريعات الغربية والعربية بخصوص موقفها من جريمة الإرهاب الإلكتروني.

الحدود الزمانية:

جرت الدراسة في العام الدراسي 2017/2016

الحدود الموضوعية:

بحثت هذه الدراسة في مفهوم جريمة الإرهاب الإلكتروني في التشريع الأردني.

منهج الدراسة:

تناولت هذه الدراسة الجرائم الالكترونية بشكل عام وجرائم الارهاب الالكتروني بشكل خاص بمنهج وصفي تحليلي مقارن يقوم على وصف ظاهرة الجرائم الالكترونية وجرائم الارهاب الالكتروني، وشرح وتحليل النصوص الجزائية الاردنية المتعلقة بالارهاب الالكتروني، للتعرف والوقوف على مواطن القوة والضعف في منهج المشرع الاردني لمعالجة الارهاب الالكتروني بالمقارنة مع التشريعات الاخرى.

تمهيد:

يوصف العصر الذي نعيشه بعصر التقنية، عصر وسائل ونقل البيانات التي غدت المحدد الاستراتيجي للبناء الثقافي والإنجاز الاقتصادي، عصر تميز باختراعات هائلة على المستوى التقني لعل من أهمها وأكثرها فائدة ظهور الحاسوب وتقنية الاتصالات، وقد أصبحت تقنية المعلومات في هذا القرن من لوازم الحياة المتطورة سواءً على المستوى العام أم الخاص، ولا يخفى أن لكل تطور تقني انعكاساته على المستوى القانوني بصفة عامة ، وفي إطار القانون الجزائي على وجه الخصوص، فكل المخترعات الحديثة تثير مسألة حمايتها جزائيا [2].

وقد قسم قانون الجرائم الالكترونية الاردني[3] الجرائم الالكترونية الى نوعين هما:

1. الجرائم الواقعة على انظمة المعلومات او محتوياتها.
2. الجرائم الواقعة باستخدام انظمة المعلومات كأداة لارتكاب الجريمة.

([2]) محمد فواز مطالقة، النظام القانوني لعقود إعداد برامج الحاسوب، ط1، دار الثقافة، عمان،2004، ص 11.

[3] المذكرة الايضاحية لقانون الجرائم الالكترونية الاردني رقم (18) لسنة 2015.

AJSP
المجلة العربية للنشر العلمي
العدد الثامن والعشرون
تاريخ الإصدار: 2 – شباط – 2021 م
www.ajsp.net
ISSN: 2663-5798

وعليه تم تقسيم هذه الدراسة الى ثلاثة مباحث على النحو التالي:

المبحث الاول: مفهوم الجرائم الالكترونية.

المبحث الثاني: خصائص الجرائم الالكترونية.

المبحث الثالث: ماهية جرائم الارهاب الالكتروني.

المبحث الاول

مفهوم الجرائم الالكترونية

إن الانتشار الواسع للحواسيب الآلية ادى إلى ظهور نوع جديد من الجرائم وهو القائم على الاستغلال غير المشروع لهذه التكنولوجيا، وهو ما يسمعى بجرائم الحاسب الآلي أو جرائم الإرهاب الإلكتروني، الأمر الذي انعكس على موضوع النظرية التقليدية في الجريمة والجزاء، إذ وفرت هذه التكنولوجيا طرقاً ووسائل جديدة لارتكاب الجرائم دون ترك اي اثر أو بذل أي جهد يذكر وذلك من خلال إدخال أوامر مختصرة وبسيطة للحاسب الآلي ومن ثم يقوم هذا الحاسب بالمهمة المطلوبة منه[4].

والجريمة تعد ظاهرة إنسانية اصيلة وجدت مع وجود الإنسان، بنوازع الخير والشر في ذاته العميقة، تكشف عنها سلوكيات خارجية يعبر بها الإنسان عن بواطن نفسه ورغباته، خيراً بخير وشراً بمثله، وقد ظهرت تعريفات عدة للجريمة، ومن هذه التعريفات المفهوم الاجتماعي للجريمة، حيث عرفت بأنها: كل فعل أو امتناع يتعارض مع القيم والأفكار التي استقرت في كيان الجماعة، أو أنها تلك التي تتعارض مع الأساسيات الخاصة بحفظ المجتمع وبقاءه"[5].

أما المفهوم القانوني للجريمة، فهي: فعل غير مشروع إيجابي أو سلبي صادر عن إرادة جنائية يقرر القانون لمرتكب هذا الفعل عقوبة أو تدبيراً احترازياً[6].

ويرى الباحث أن مفهوم الجريمة هنا إنما يركز على محورين أساسيين لتمييز الجريمة الجزائية؛ الأول الاستناد إلى نص جزائي يقرر تجريم فعل أو امتناعاً سلبياً كان أم إيجابياً وفق لمبدأ شرعية الجريمة "لا جريمة ولا عقوبة إلا بنص" هذا النص مكانه الطبيعي قانون العقوبات العام، لكن لا يعني هذا عدم إمكان ورود نص التجريم في غيره من القوانين، أما الأساس الثاني فهو يتعلق بالعقوبة الذي يضعه المشرع جزاءاً لمخالفة أمره ويجب أن يتصف بالطبيعة الجزائية، فلا يخرج عن أمرين عقوبة أو تدبير احترازي.

المطلب الأول: تعريف البيانات والمعلومات

المعلومات لغة، هي جمع معلومة وهي مشتقة من الفعل علم ومعناه المعرفة ويقال أعلم فلاناً الخبر بمعنى أخبره به وأعلم فلاناً الأمر بمعنى جعله يعرفه.[7]

يستخدم مصطلح نظم المعلومات في الفقه القانوني للدلالة على المعنى المقصود نفسه بهذا المصطلح وفقا لمفهومه العلمي، فهي مجموعة عناصر مادية وغير مادية يمكن باجتماعها التعامل مع المعلومة[8].

---

[4] المناعسة، أسامة والزعبي ، جلال، والهواوشة ، صايل (2001) جرائم الحاسب الآلي والانترنت، دراسة تحليلية مقارنة، دار وائل للنشر، عمان، ص9

[5] رمسيس، بهنام (1981)، النظرية العامة للقانون الجنائي، منشأة المعارف، الإسكندرية، ص52–53.

[6] نجم، محمد صبحي (1988)، شرح قانون العقوبات الإردني، القسم العام، منشورات الجامعة الأردنية، عمان، ص65.

[7] إبراهيم مصطفى: المعجم الوسيط، ج2،ط3، مجمع اللغة العربية، القاهرة، 1985، ص647.

[8] خالد حمدي: الحماية القانونية للكيانات المنطقية (برامج المعلومات)، رسالة دكتوراة، جامعة عين شمس، 1992، ص39، محمد فواز مطالقة، النظام القانوني لعقود إعداد برامج الحاسوب، مرجع سابق، ص 11.

العدد الثامن والعشرون
تاريخ الإصدار: 2 – شباط – 2021 م
www.ajsp.net
ISSN: 2663-5798

أولا: المعلومات والبيانات: إن مصطلحات المعلومات والبيانات والمعطيات تستخدم كألفاظ مترادفة في المجال القانوني لعدم وجود أهمية في التمييز فيما بينها طالما أن المعلومات هي النتيجة المستخلصة من البيانات أو المعطيات فكلاهما يتمتع بالحماية القانونية نفسها[9]، واستناداً لهذه الاعتبارات ولتجنب استخدام ألفاظ متكررة في البحث دون جدوى فإن الباحث سوف يكتفي باستخدام مصطلح المعلومات للدلالة على النتيجة المستخلصة من البيانات وكمعنى مرادف لهذه البيانات

المطلب الثاني: اقسام البيانات والمعلومات

مفهوم المعلومات:

عرف المشرع الاردني البيانات والمعلومات في المادة (2) من قانون جرائم أنظمة المعلومات لعام 2010 على أنها: " المادة2– يكون للكلمات والعبارات التالية حيثما وردت في هذا القانون المعاني المخصصة لها أدناه ما لم تدل القرينة على غير ذلك:–

نظام المعلومات: مجموعة البرامج والأدوات المعدة لإنشاء البيانات أو المعلومات إلكترونيا، أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو إداراتها.

البيانات: الأرقام والحروف والرموز والأشكال والأصوات والصور التي ليس لها دلالة بذاتها.

المعلومات: البيانات التي تمت معالجتها وأصبح لها دلالة.

ويعرف بعض الباحثين المعلومات بأنها "تعبير عن الأفكار بصيغة بيانات أو نصوص أو صور أو أشكال أو أصوات أو رموز أو قواعد بيانات أو برامج حاسب وما شابه ذلك يتم معالجتها بحيث تعطي معنى يؤدي إلى إيجاد معرفة أو تطويرها حسب الأصول".[10]

2. أقسام المعلومات:

1. النوع الأول: المعلومات الاسمية: يقصد بها المعلومات التي تسمح بشكل مباشر أو غير مباشر بالتعريف على الشخص موضوع المعلومة أو تجعله قابلاً للتعرف عليه، وهي تقسم إلى قسمين:

- المعلومات الشخصية وهي المعلومات المرتبطة بشخص المخاطب بها مثل اسمه وحالته الاجتماعية وموطنه، وهي لا تعكس آراء شخصية للغير بل تتعلق ببيانات مجردة، وتتمتع هذه المعلومات بخاصية السرية فلا يجوز للغير الاطلاع عليها إلا بموافقة أو بإذن السلطات المختصة.
- المعلومات الموضوعية: وهي المعلومات التي تحمل رأياً ذاتياً عن الغير مثل تقارير كفاية الموظفين التي يضعها الرؤساء لتقييم المرؤوسين، وهذه المعلومات تتفق مع المعلومات الشخصية في أنها خاصة بشخص محدد إلا أنها تختلف عنها في أنها موجهة إلى الغير وليس إلى شخص صاحبها.

2. النوع الثاني: المعلومات المبتكرة: يقصد بها المعلومات التي يتمتع مالكها بحقوق الملكية الفكرية كحقوق التأليف على المصنفات الفنية والأدبية أو حقوق الاختراع على الملكية الصناعية حيث يتمتع مالكوها بحقوق استئثارية باستغلالها.[11]

3. النوع الثالث: المعلومات المباحة: ويقصد بها المعلومات التي يتاح للجميع الحصول عليها بحيث لا يكون لها مالك يتمتع بحقوق استئثارية عليها ومن أمثلتها الأخبار العامة والتشريعات.[12]

---

[9] محمد حسام لطفي: عقود خدمات المعلومات، ط1، بدون ناشر، القاهرة، 1994، ص15–16. د. نائلة قورة: جرائم الحاسب، مرجع سابق، ص94.

[10] فادي فلاح: رسالة المعلومات الإلكترونية في القانون الأردني، رسالة ماجستير، الجامعة الأردنية 2004، ص36–37.

[11] ماجد عمار: المسؤولية القانونية الناشئة عن استخدام فيروس برامج الكمبيوتر ووسائل حمايتها، ط1، دار النهضة العربية، القاهرة، 1989، ص 76–77.

[12] ماجد عمار: المسؤولية القانونية الناشئة عن استخدام فيروس برامج الكمبيوتر ووسائل حمايتها مرجع سابق ، ص161.

العدد الثامن والعشرون
تاريخ الإصدار: 2 – شباط – 2021 م
www.ajsp.net
ISSN: 2663-5798

ثانيا: برامج الحاسوب: ويعرف برنامج الحاسوب من الناحية العلمية بأنه "تعليمات متتالية تصف العمل المطلوب إنجازه بوساطة جهاز الحاسوب"

ثالثا: قواعد البيانات: تعرف قواعد البيانات بمفهومها العلمي بأنها " مجموعة كبيرة من البيانات موضوعة بطريقة منظمة بحيث يمكن الوصول إليها بسهولة وإجراء العمليات المختلفة عليها".[13]

ويعرف الفقه القانوني قواعد البيانات على نحو مماثل لتعريفها العلمي بأنها "مجموعة بيانات مسجلة في ملفات على نحو يحدد الروابط المنطقية بين نوعياتها المختلفة وبفضلها يتم استرجاع مخزون البنك من المعلومات بسهولة ويسر عن طريق الحاسبات"[14]ويتوجب التمييز بين قاعدة البيانات والتي تمثل نظاماً لإدارة البيانات المخزنة في الحاسوب وبوساطتها يتم إدخال المعلومات واسترجاعها وبين البيانات ذاتها وهي ما يتم تخزينه في الحاسوب من خلال قاعدة البيانات والرجوع إليه من خلالها.[15]

غير أن كلا من البيانات وقواعد البيانات يدخل في مفهوم المعلومات من الناحية العلمية والقانونية كما سبقت الإشارة ويخضعان للنظام القانوني نفسه في الحماية في إطار جريمة الإتلاف.

ويمكن تعريف الجريمة الإلكترونية بأنها: "كل عمل أو امتناع يأتيه الإنسان أضراراً بمكونات الحاسب الآلي أو شبكات الاتصال الخاصة به والتي يحميها قانون العقوبات ويفرد لها عقاباً"[16].

كما يمكن تعريفها بأنها جرائم يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسوب بعمل غير قانوني[17].

المبحث الثاني

خصائص الجرائم الالكترونية

نظراً لارتباط الجريمة الإلكترونية بجهاز الحاسوب، وشبكة الإنترنت بصفة عامة، ووسائل التواصل الاجتماعي بصفة خاصة، فقد أضفى عليها ذلك مجموعة من الخصائص المميزة لها عن خصائص الجريمة التقليدية.

ولمزيد من التفصيل سيتم تناول الفصل من خلال المطلبين التاليين:

المطلب الأول: سمات أو ميزات الجرائم الالكترونية

المطلب الثاني: سمات أو مميزات مرتكبي الجرائم الالكترونية

المطلب الاول: سمات أو ميزات الجرائم الالكترونية

الجرائم الإلكترونية جريمة مستحدثة: تعدّ الجرائم الإلكترونية من أبرز أنواع الجرائم الجديدة التي يمكن أن تشكل أخطاراً جسيمة في ظل العولمة، فلا غرابة أن تعدّ الجرائم الإلكترونية – سواء التي تتعرض لها أجهزة الكمبيوتر أو التي تسخر تلك الأجهزة في ارتكابها – من الجرائم المستحدثة، حيث إن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة، بحيث

---

[13] علي بهلوان: استخدام قاعدة البيانات ومنتج التطبيقات، دار الكتب العلمية للنشر والتوزيع، ط2، القاهرة، ص 21.

[14] محمد حسام لطفي: عقود خدمات المعلومات، مرجع سابق، ص 12.

[15] محمد علي الزعبي: الحماية القانونية لقواعد البيانات وفقا لقانون حماية حق المؤلف، ط1، منشأة المعارف، الاسكندرية، 2003، ص 78 وما بعدها.

[16] رستم ، هشام (1995)، جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة، ورقة عمل مقدمة إلى اللجنة العلمية لإعداد التقرير الوطني المصري لمؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاقبة المجرمين، مجلة الدراسات القانونية، جامعة أسيوط، عدد 17، القاهرة، ص22.

[17] اليوسف، عبد العزيز (1999)، التقنية في الجرائم المستحدثة، بحث ضمن كتاب الظواهر الإجرامية المستحدثة وسبل مواجهتها، منشورات أكاديمية نايف للعلوم الأمنية ، الرياض، ص218.

العدد الثامن والعشرون
تاريخ الإصدار: 2 – شباط – 2021 م
www.ajsp.net
ISSN: 2663-5798

يتجاوز هذا التقدم بقدراته وإمكاناته أجهزة الدولة الرقابية، بل إنه أضعف من قدراتها في تطبيق قوانينها، بالشكل الذي أصبح يهدد أمها وأمن مواطنيها[18].

جرائم عابرة للحدود: أعطى انتشار شبكة الإنترنت إمكانية لربط أعداد هائلة من أجهزة الحاسوب المرتبطة بالشبكة العنكبوتية من غير أن تخضع لحدود الزمان والمكان، لذلك فإن من السهولة بمكان أن يكون المجرم في بلد ما والمجني عليه مقيم في بلد آخر، وهنا تظهر الحاجة لوجود تنظيم قانوني دولي وداخلي متلائم معه لمكافحة مثل هذا النوع من الجرائم وضبط فاعليها، وحيث إن التشريعات الداخلية متفاوتة فيما بين كل دولة من دول العالم، تظهر العديد من المشاكل حول صاحب الاختصاص القضائي لهذه الجريمة وإشكالات أخرى متعلقة بإجراءات الملاحقة القضائية، وتتشابه الجرائم الإلكترونية في هذه الخاصية مع بعض الجرائم مثل جرائم غسيل الأموال، وجرائم المخدرات[19].

جرائم صعبة الإثبات: تمتاز الجرائم الالكترونية بالتباعد الجغرافي الذي يثير الإشكال بدايةً، حيث تشير الدراسات أن ما يتم اكتشافه من جرائم المعلومات يصل إلى نسبة 1% والذي يتم الإبلاغ عنه من هذه النسبة لا يكاد يصل إلى 5% فقط[20].

والوسيلة المستخدمة لارتكاب الجريمة هي نبضة إلكترونية ينتهي دورها خلال أقل من ثانية واحدة، وكأن الجاني يقوم بتدمير الدليل بمجرد استعماله ويقوم بذلك بكل هدوء ودون إحداث أية ضجة، وذلك على خلاف الكثير من الجرائم التي نعرف[21].

جرائم مغرية للمجرمين[22]: نظراً للصفات التي تتمتع بها مثل هذه الجريمة، والصعوبات التي تثور عند محاولة اكتشافها أو ملاحقتها، فإن ذلك يشكل إغراءً كبيراً للمجرمين وخصوصاً أنه يمكن تحقيق مكاسب طائلة من وراء مثل هذا النوع من الجرائم، ونتيجة لكل ما سبق تعد مثل هذه الجرائم جريمة تستهوي الكثيرين لسهولتها، وكثرة مكاسبها، بالاضافة إلى وجود رغبة لدى البعض في تحدي الحاسوب.

وقوع الجرائم الإلكترونية أثناء المعالجة الآلية للبيانات: من خصائص الجريمة الإلكترونية أنها تقع أثناء عملية المعالجة الآلية للبيانات والمعطيات الخاصة بالكمبيوتر، ويمثل هذا النظام الشرط الأساسي الذي يتعين توافره حتى يمكن البحث في قيام أو عدم قيام أركان الجريمة الإلكترونية الخاصة بالتعدي على نظام معالجة البيانات، ذلك أنه في حالة تخلف هذا الشرط تنتفي الجريمة الإلكترونية[23].

"وقد كان هناك اقتراح من قبل مجلس الشيوخ الفرنسي حال تعديل قانون العقوبات الحالي، بوضع تعريف محدد لعملية المعالجة الآلية للبيانات أو المعطيات، ولكن حذف هذا التعريف باعتبار أنها عملية فنية تخضع للتطور السريع، وبالتالي سيكون أي تعريف لها قاصراً، وكان هذا التعريف ينص على أنها: "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، والتي تتكون كل منها من

([18]) إبراهيم، خالد ممدوح، مرجع سابق، ص86.

([19]) القطاونة، مصعب (2010). الإجراءات الجنائية الخاصة في الجرائم المعلوماتية، بحث مقدّم لشبكة قانوني الأردن، ص5.

([20]) القطاونة، مصعب، مرجع سابق، ص6.

([21]) المطردي، مفتاح بو بكر، مرجع سابق، ص8.

([22]) عبابنة، محمود أحمد، مرجع سابق، ص30.

([23]) قورة، نائلة، مرجع سابق، ص55.

العدد الثامن والعشرون
تاريخ الإصدار: 2 – شباط – 2021 م
www.ajsp.net
ISSN: 2663-5798

الذاكرة، والبرامج، والمعطيات، وأجهزة الإدخال، والإخراج، وأجهزة الربط، والتي يربط بينها مجموعة من العلاقات والتي عن طريقها يتم تحقيق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضعاً لنظام الحماية الفنية"[24].

والجريمة الإلكترونية قد تقع أثناء عملية المعالجة الآلية للبيانات في أي مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلي للبيانات سواء عند مرحلة إدخال البيانات، أو أثناء مرحلة المعالجة، أو أثناء مرحلة إخراج المعلومات.

احتمال تعدد الأوصاف القانونية لمحل الجريمة الإلكترونية: إن محل الجريمة الإلكترونية قد يظهر بمظهرين أحدهما مادي والثاني معنوي، كما هو الحال بالنسبة للمعلومات فقد تكون في حالة انتقال أو موجودة في ذاكرة النظام الإلكتروني أي أنها في حالة غير مادية، والشكل الآخر أن تكون المعلومات متجسدة في صورة مادية بتخزينها على دعامة إلكترونية، حتى أن المعلومات غير المادية بطبيعتها يمكن أن تخضع لأكثر من نص قانوني، وفقاً لما إذا كانت في شكل مادي أو غير مادي، وفي الشكل الأخير يوجد لها أكثر من نص قانوني يمكن أن تخضع له، مثال ذلك اعتبارها مصنف أدبي مما يثير مشكلة تعدد الأوصاف القانونية على ذات المحل[25].

المطلب الثاني: سمات أو مميزات مرتكبي الجرائم الالكترونية

يتميز الفاعل في الجريمة الإلكترونية بعدد من السمات والخصائص، هي: أنه يتمتع بالمهارة والمعرفة والذكاء، كما أنه إنسان اجتماعي، كذلك يعمل على تبرير ارتكاب جريمته وفي الوقت ذاته يتولد لديه شعور بالخوف من كشف جريمته، كما أن الفاعل في هذه الجريمة يتمتع بالسلطة تجاه النظام الإلكتروني.

وقد لا تتأثر الجرائم التقليدية بالمستوى العلمي للمجرم كقاعدة عامة، ولكن الأمر مختلف تماماً بالنسبة للمجرم المعلوماتي والذي يكون عادة من ذوي الاختصاص والمعرفة في مجال تقنية المعلومات.

وقد تمّ تصنيف مجرمي الجرائم الإلكترونية إلى المخترقين والمحترفين والحاقدين.

أ. **المخترقون:** مثل الهاكرز الذي يعدّ شخصاً بارعاً في استخدام الحاسب الآلي ولديه فضول في استخدام حسابات الآخرين بطرق غير مشروعة، الأمر الذي يدل على أنهم أشخاص متطفلون وغير مرحب بهم لدى الغير، وأغلبهم ما يكون جانبهم تحدي الشباب للدخول إلى المواقع الرسمية، وبعض الأحيان الدخول إلى مواقع الحسابات من أجل إثبات الذات، وغالباً تكون أعمارهم في سن المراهقة[26].

ب. **المحترفون:** وهم الأكثر خطورة بين مجرمي الإنترنت، حيث يهدف البعض منهم إلى الاعتداء لتحقيق الكسب غير المشروع المتمثل في الناحية المادية وذلك عبر الدخول في حسابات البنوك، والبعض الآخر يدخل من أجل تحقيق أغراض سياسية والتعبير عن وجهة نظره أو فكرة، وغالباً أعمال هؤلاء تكون بين 25 و 40 سنة[27].

ج. **الحاقدون:** وهم الذين ليس لديهم أي أهداف للجريمة ولا يسعون لمكاسب سياسية أو مادية ولكن يتحركون لرغبة في الانتقام والتأثر كالأمور الطائفية[28].

([24]) نقلاً عن: القهوجي، علي عبد القادر (2000). الحماية الجنائية للبيانات المعالجة إلكترونياً، بحث مقدّم إلى مؤتمر القانون والكمبيوتر والإنترنت والذي عُقد خلال الفترة من 1–3 مايو، كلية الشريعة والقانون، جامعة الإمارات العربية، ص43.

([25]) إبراهيم، خالد ممدوح، مرجع سابق، ص87–88.

([26]) قورة، نائلة عادل (2012). جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، ط1، ص178.

([27]) إبراهيم، خالد ممدوح (2009). الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط1، ص78.

([28]) إبراهيم، خالد ممدوح، مرجع سابق، ص79.

العدد الثامن والعشرون
تاريخ الإصدار: 2 – شباط – 2021 م
www.ajsp.net
ISSN: 2663-5798

المبحث الثالث

ماهية جرائم الارهاب الالكتروني

إن الاستغلال المتعسف للحاسوب والإنترنت والانتشار الواسع لها ، أظهر أنواعا جديدة من الجرائم القائمة على الاستغلال غير المشروع لهذه التكنولوجيا، أصطلح على تسميتها بالجرائم المعلوماتية أو جرائم الحاسوب ، وهذه التكنولوجيا الحديثة أدت إلى ثورة هائلة وانقلاب خطير في النظرية التقليدية للجريمة والجزاء، إذ وفرت طرق ووسائل جديدة للأشخاص لارتكاب جرائمهم ، دون أن يتركوا أثرا أو يتحملوا جهودا كبيرة ، خصوصا باعتماد الغالبية العظمى من هذه الجرائم على إدخال أوامر مختصرة وبسيطة للحاسب الآلي ليتكفل هو بعد ذلك بالباقي .

إن ظاهرة جرائم الحاسوب أو الجريمة الإلكترونية، ظاهرة مستجدة نسبيا توجب على البشرية التنبه لأهمية وحجم المخاطر والخسائر الناجمة عنها ، باعتبارها تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة (المعلومات والبيانات والبرامج بكافة أنواعها) ، في جريمة تقنية تنشأ في الخفاء ، يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية التي توجه للنيل من الحق في المعلومات ، وتطال اعتداءاتها معطيات الحاسوب المخزنة والمنقولة عبر أنظمة وشبكات الحاسوب وفي مقدمتها الإنترنت ، وأجهزة الحاسوب نفسها مما يخلق مشاكل قانونية وخسارة مادية هائلة .

يمكننا تعريف الإرهاب الإلكتروني بأنه: العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان، في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق ,باستخدام المواد المعلوماتية والوسائل الإلكترونية بشتى صنوف العدوان وصور الإفساد. [29]

فالإرهاب الإلكتروني يعتمد على استخدام الإمكانيات العلمية والتقنية, واستغلال وسائل الاتصال والشبكات المعلوماتية, من أجل تخويف وترويع الآخرين, وإلحاق الضرر بهم, أو تهديدهم.

خصائص الارهاب الالكتروني

يتميز الإرهاب الإلكتروني بعددٍ من الخصائص والسمات التي يختلف فيها عن بقية الجرائم, وتحول دون اختلاطه بالإرهاب العادي, ومن الممكن إيجاز أهم تلك الخصائص والسمات فيما يلي:

1. إن الإرهاب الإلكتروني لا يحتاج في ارتكابه إلى العنف والقوة, بل يتطلب وجود حاسب آلي متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة.
2. يتسم الإرهاب الإلكتروني بكونه جريمة إرهابية متعدية الحدود, وعابرة للدول والقارات, وغير خاضعة لنطاق إقليمي محدود.
3. صعوبة اكتشاف جرائم الإرهاب الإلكتروني, ونقص الخبرة لدى بعض الأجهزة الأمنية والقضائية في التعامل مع مثل هذا النوع من الجرائم.
4. صعوبة الإثبات في الإرهاب الإلكتروني, نظراً لسرعة غياب الدليل الرقمي, وسهولة إتلافه وتدميره.
5. يتميز الإرهاب الإلكتروني بأنه يتم عادة بتعاون أكثر من شخص على ارتكابه.
6. أن مرتكب الإرهاب الإلكتروني يكون في العادة من ذوي الاختصاص في مجال تقنية المعلومات, أو على الأقل شخص لديه قدر من المعرفة والخبرة في التعامل مع الحاسب الآلي والشبكة المعلوماتية.

([29]) عصام عبد الفتاح مطر: الجريمة الإرهابية، دار الجامعة الجديدة، الاسكندرية، 2008م، ص2.

العدد الثامن والعشرون
تاريخ الإصدار: 2 – شباط – 2021 م
www.ajsp.net
ISSN: 2663-5798

المطلب الاول: اركان جريمة الارهاب الالكتروني

تقوم الجريمة بشكل عام على أركان ثلاثة، هي[30]:

الركن الشرعي: وهو الصفة غير المشروعة للفعل، وتتمثل قاعدة التجريم والعقاب للجرائم الالكترونية في ما ورد النص عليه في قانون جرائم انظمة المعلومات الاردني.

الركن المادي: وهو ماديات الجريمة التي تبرز به الى العالم الخارجي.

الركن المعنوي: وهو الارادة التي يقترن بها الفعل سواء في صورة القصد او الخطأ.

الركن الشرعي لجريمة الارهاب الالكتروني

ولقد توسع المشرع الأردني في تعريف الجريمة الإرهابية وحاول في هذا التعريف إضافة صور أخرى للتجريم، ولقد نجح المشرع الأردني في القانون المعدل ومن خلال تعريفه للجريمة الإرهابية بالجمع بين التأثير النفسي وهو إدخال الرعب والخوف والتأثير المادي الناتج من العمل الإرهابي. لهذا ومن خلال المادة (147) من قانون العقوبات الأردني والتي تنص على: "1- يقصد بالإرهاب: استخدام العنف بأي وسيلة كانت أو التهديد باستخدامه ، أياً لمشروع اجرامي فردي أو جماعي يهدف الى تعريض سلامة المجتمع وأمنه للخطر إذا كان من يقع تنفيذا شأن ذلك إلقاء الرعب بين الناس وترويعهم أو تعريض حياتهم للخطر أو الحاق الضرر بالبيئة أو المرافق والأملاك العامة أو الأملاك الخاصة أو المرافق الدولية او البعثات الدبلوماسية أو باحتلال أي منها أو الاستيلاء عليها أو تعريض الموارد الوطنية للخطر او ارغام أي حكومة او أي منظمة دولية او اقليمية على القيام بأي عمل او الامتناع عنه.

ويعاقب من يرتكب هذه الجريمة بالأشغال الشاقة المؤقتة ويعاقب الإداري المسؤول في البنك أو المؤسسة المالية الذي أجرى العملية وهو عالم بذلك بالحبس ، وتتم مصادرة الأموال التي تم التحفظ عليها.

جرم المشرع الأردني من خلال نص المادة (1/148) المؤامرة لارتكاب أعمال إرهابية، ولقد عرف المشرع الأردني جريمة المؤامرة في المادة (107) من قانون العقوبات[31].

وفرض المشرع عقوبة الأشغال الشاقة المؤقتة من (3-15) لمرتكبي هذا العمل الإرهابي، وفي بيان عناصر المؤامرة فقد قررت محكمة التمييز بقرارها 2004/958 والذي جاء فيه: (تتمثل عناصر جريمة المؤامرة بقصد القيام بأعمال إرهابية في التقاء إرادة شخصين أو أكثر وتفاهمهم على أمر معين وأن يكون موضوع هو ارتكاب أعمال إرهابية ترمي إلى إيجاد حالة ذعر وترتكب بوسائل معينة من أن تحدث خطراً...).

وفي الفقرة الثانية من المادة (148) فقد جرم المشرع الأعمال الإرهابية الخالية من التشديد بأن جعل عقوبتها الأشغال الشاقة لمدة خمس سنوات على الأقل.

فالأعمال الإرهابية ذات خطورة عالية، وتمتاز بعقوبات قاسية على مرتكبيها، ويجب التأكد من أن ملابسات الفعل ترتقي إلى صفة العمل الإرهابي[32].

أما الجرائم الإرهابية ذات العقوبة المشددة وهي الأشغال الشاقة المؤبدة فقد بينها المشرع في الفقرة الثالثة من المادة (148)، ولتحقق التشديد فقد تطلب المشرع أن ينتج عن العمل الإرهابي ما يلي:

---

[30] الجبور، محمد (2012) الوسيط في قانون العقوبات- القسم العام، دار وائل للنشر والتوزيع، عمان، ط1، ص59

([31]) نص المادة (107): المؤامرة في كل اتفاق تم بين شخصين أو أكثر على ارتكاب جريمة بوسائل معينة.

([32]) انظر بهذا المعنى قرار محكمة التمييز الأردنية بصفتها الجزائية رقم 2007/653 بتاريخ 2007/10/21 منشورات شبكة قانوني الأردن

أ- إلحاق الضرر، ولو جزئياً، في بناية عامة أو خاصة أو مؤسسة صناعية أو سفينة أو طائرة أو أي وسيلة نقل أو أية منشآت أخرى.

ب- تعطيل سبل الاتصال وأنظمة الحاسوب أو اختراق شبكاتها أو التشويش عليها أو تعطيل وسائط النقل أو إلحاق الضرر بها كلياً أو جزئياً.

كما نصت المادة رقم (2) من قانون منع الارهاب الاردني رقم 18 لسنة 2014 " العمل الارهابي : كل عمل مقصود يرتكب باي وسيلة كانت يؤدي الى قتل اي شخص او التسبب بايذائه جسديا او ايقاع اضرار في الممتلكات العامة او الخاصة او في وسائط النقل او البيئة او في البنية التحتية او في مرافق الهيئات الدولية او البعثات الدبلوماسية اذا كانت الغاية منه الاخلال بالنظام العام وتعريض سالمة المجتمع وامنه للخطر او تعطيل تطبيق احكام الدستور او القوانين او التأثير على سياسة الدولة او الحكومة او اجبارها على عمل ما او الامتناع عنه او الاخلال بالامن الوطني بواسطة التخويف او الترهيب او العنف. "

وبمطالعة النص اعلاه نجد انه لم يحدد وسيلة معينة لارتكاب العمل الارهابي سواء وسيلة تقليدية ام الكترونية.

وبالعودة الى نص المادة (3/أ) من قانون منع الارهاب الالكتروني الاردني رقم 18 لسنة 2014 فقد نصت على: "مع مراعاة احكام قانون العقوبات النافذ المفعول ، تحظر الاعمال الارهابية ويعتبر في حكمها الاعمال التالية

أ. القيام باي وسيلة كانت مباشرة او غير مباشرة ، بتقديم او جمع او تدبير الاموال بقصد استخدامها لارتكاب عمل ارهابي او مع العلم انها ستستخدم كليا او جزئيا سواء اوقع او لم يقع العمل المذكور داخل المملكة او ضد مواطنيها او مصالحها في الخارج. "

وبمطالعة النص نجد ان المشرع الاردني فيما يختص بالاعمال الارهابية بين انها تكون من خلال القيام باي وسيلة كانت مباشرة او غير مباشرة وبالتالي تصبح شبكة الانترنت داخلة ضمن الوسائل التي تؤدي الى القيام بتقديم او جمع او تدبير الاموال بقصد استخدامها لارتكاب عمل ارهابي.

كما وانه ومن خلال استطلاع نص المادة (10) من قانون جرائم انظمة المعلومات الاردني المؤقت لسنة 2010

"المادة 10 – كل من استخدم نظام المعلومات أو الشبكة المعلوماتية أو انشأ موقعاً الكترونياً لتسهيل القيام بأعمال إرهابية أو دعم لجماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية أو الترويج لإتباع أفكارها، أو تمويلها يعاقب بالأشغال الشاقة المؤقتة."

يتبين لدينا ان القانون نص على ان كل من قام باعمال ارهابية فانه يعاقب بالاشغال الشاقة المؤقتة وقد تم الغاء هذا النص بسبب صدور قانون منع الارهاب الالكتروني رقم (18) لعام 2014.

وبالنظر الى نص المادة (15) من قانون الجرائم الالكترونية الجديد:

"المادة 15: كل من ارتكب أي جريمة معاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتية أو أي نظام معلومات أو موقع الكتروني أو اشترك أو تدخل أو حرض على ارتكابها، يعاقب بالعقوبة المنصوص عليها في ذلك التشريع."

ومن خلال استطلاع المادة نجد انها من باب التجريم الخوفي فأي جريمة تقليدية ترتكب باستخدام الشبكة المعلوماتية يعاقب عليها بالعقوبة المعنون عليها في ذلك التشريع.

المطلب الثاني: القصد الجرمي في الجرائم المقصودة

تعد جريمة إتلاف نظم المعلومات من الجرائم العمدية والأصل أن يتخذ الركن المعنوي فيها صورة القصد ، وفي هذه الحالة يتطلب تمام الركن المعنوي توافر القصد العام لدى الجاني، إلا أن بعض التشريعات تشترط توافر قصد خاص لدى الجاني إلى جانب القصد العام، ونبحث فيما يلي نوعي القصد المذكورين:

العدد الثامن والعشرون
تاريخ الإصدار: 2 – شباط – 2021 م
www.ajsp.net
ISSN: 2663-5798

القصد العام

يتطلب ثبوت القصد العام في جريمة إتلاف نظم المعلومات توافر عنصرين وهما العلم والإرادة ، ويقتضي ثبوت علم الجاني بأن نظام المعلومات محل جريمة الإتلاف مملوك للغير وأن من شأن فعله التأثير على مادته أو قيمته، وكذلك يتوجب أن تتجه إرادته إلى إحداث الإتلاف أو التعطيل في نظام المعلومات.

ولكن هل يشترط لتوفر القصد العام أن تتجه إرادة الفاعل إلى إحداث الضرر في نظام المعلومات ام يكفي لتوفره اتجاه الإرادة إلى إحداث التعديل أو المحو أو الإدخال في نظام المعلومات ولو لم تتوافر فيه إحداث الضرر؟

يرى اتجاه في الفقه وجوب توافر نية إحداث الضرر كنتيجة للسلوك الجرمي لأغراض ثبوت القصد الجرمي لدى مرتكب جريمة إتلاف المعلومات تطبيقاً للقواعد العامة التي تقتضي اتجاه إرادة الفاعل لإحداث النتيجة الجرمية كعنصر يلزم توافره لثبوت القصد الجرمي بينما يرى اتجاه آخر عكس ذلك.

ويرى الباحث أنه ينبغي التمييز هنا بين جرائم الإتلاف التي يشترط فيها القانون تحقق النتيجة الجرمية وبين الجرائم التي يكتفي فيها القانون بارتكاب السلوك المجرد.

ففي الجرائم ذات النتيجة الجرمية يتوجب أن تتجه إرادة الفاعل إلى تحقيق النتيجة الجرمية لقيام القصد باعتبار أن هذه النتيجة تمثل عنصرا في الركن المادي للجريمة، أما في جرائم الخطر فالقصد الجرمي يتوفر فيها بمجرد اتجاه إرادة الفاعل إلى ارتكاب السلوك المكون لركنها المادي[33] .

وقد نصت المادة (63) من قانون العقوبات الليبي على المبدأ المتقدم صراحة بقولها " ترتكب الجناية أو الجنحة عن قصد عمدي إذا كان مقترفها يتوقع ويريد أن يترتب على فعله أو امتناعه حدوث الضرر أو وقوع الخطر الذي حدث والذي يعلق عليه القانون وجود الجريمة"[34].

وقد اتجه القضاء المقارن في الدول التي تكتفي تشريعاتها بارتكاب السلوك المجرد في تجريم إتلاف نظم المعلومات إلى عدم اشتراط توافر نية الضرر لدى الجاني، ففي قضية تتلخص وقائعها بأن أحد الموظفين قام بتعديل معلومات التي سبق وأن قام بتسجيلها بطريقة نهائية في نظام آلي للمحاسبة كان يقوم بالإشراف عليه، وقد قررت محكمة النقض الفرنسية تأييد الحكم الاستئنافي بإدانة المتهم بجريمة إلغاء والتعديل العمدي للمعلومات وقررت في هذه القضية أنه لا يشترط لتوافر الركن المعنوي في هذه الجريمة توافر نية لدى الجاني إحداث الضرر في نظام المعلومات.

وفي الولايات المتحدة اتجه القضاء الأمريكي في قضية موريس عام 1991 إلى أن القانون لا يتطلب إثبات نية الجاني بإحداث نتيجة الضرر جراء سلوكه وفي هذه القضية كان موريس قد أنتج عام 1988 برنامج الدودة بهدف إثبات عدم فاعلية الإجراءات الأمنية القائمة لحماية شبكات الحاسوب وإظهار عيوبها بنشره عبر الإنترنت وقد أدى إلى تلف أعداد كبيرة من برامج الحاسوب[35].

القصد الخاص

قد يتطلب القانون إلى جانب القصد العام المتمثل بإرادة ارتكاب الجريمة والعلم بعناصرها دافعا محدداً لارتكابها يسمى القصد الخاص والقاعدة في جرائم إتلاف نظم المعلومات إن توفر القصد العام يكفي لقيام هذه الجريمة .

([33]) الجنيهي، منير محمد، والجنيهي، ممدوح، محمد المصدر نفسه، ص78.

([34]) المادة (63) من قانون العقوبات الليبي.

([35]) الجنيهي، منير محمد، والجنيهي، ممدوح، محمد المصدر نفسه، ص80.

العدد الثامن والعشرون
تاريخ الإصدار: 2 – شباط – 2021 م
www.ajsp.net
ISSN: 2663-5798

وعلى ذلك يستوي في نظر القانون أن يكون دافع الجاني من وراء إتلاف نظم المعلومات الانتقام من مالكها أو العبث واللهو أو إثبات المقدرة على اختراق تدابير حماية نظم المعلومات، فالقاعدة أن الدافع على ارتكاب الجريمة لا يعد عنصراً من عناصر التجريم إلا في الأحوال التي ينص فيها القانون على ذلك .

فإذا قام أحد الأشخاص بزرع فيروس بهدف حماية البرنامج الذي أنتجه من خطر النسخ غير المشروع وأدى ذلك إلى إلحاق الضرر بالبيانات المخزنة في حاسوب مستخدم البرنامج فإن البرنامج هنا ليس سوى دافع على ارتكاب الجريمة وهو لا يؤثر على قيام ركنها المعنوي .

المطلب الثالث: اثبات جرائم الارهاب الالكتروني واساليب مكافحته

يعرف الأثبات: اقامة الدليل أمام القضاء بالطرق التي حددها القانون على وجود واقعة قانونية ترتبت أثارها، اي ان الدليل يقدم من قبل الخصوم امام القضاء و بالطرق المعتبرة قانوناً على وجود واقعة قانونية تختلف عليها فيما بينهم.

والهدف من الإثبات هو بيان مدى التطابق بين النموذج القانوني للجريمة وبين الواقعة المعروضة ، فإنه في سبيل ذلك يستخدم وسائل معينة هي وسائل الإثبات

أساليب مكافحة الجرائم الإلكترونية في الاتي

1. رسم سياسات دولية تفرض عقوبات صارمة على مرتكبي جرائم الإنترنت إذ يستلزم التدخل الحكومي والدولي نظراً للخطورة الجسيمة للأمر.
2. الاعتماد على أساليب وتقنيات متطوّرة للتمكن من الكشف عن هوية مرتكب الجريمة والاستدلال عليه بأقل وقت ممكن.
3. توعية الأفراد ونصحهم لماهية الجرائم الإلكترونية وكل ما يترتب عليها من مخاطر.
الحرص على الحفاظ على سرية المعلومات الخاصة بالعناوين الإلكترونية كالحسابات البنكية، والبطاقات الائتمانيّة وغيرها.
4. عدم الكشف عن كلمة السر نهائياً وتغييرها بشكل مستمر واختيار كلمات سر صعبة. تجنب تخزين الصور الخاصة بالأفراد على مواقع التواصل الاجتماعي وأجهزة الحاسوب.
5. تجنّب تحميل أي برنامج مجهول المصدر.
6. استمرارية تحديث برامج الحماية الخاصة بأجهزة الحاسوب ومنها ، MCafee, Norton.
7. تأسيس منظمة خاصة لمكافحة الجرائم الإلكترونية والحد منها.
8. المسارعة في الإبلاغ للجهات الأمنية فور التعرض لجريمة إلكترونية.
9. مواكبة التطورات المرتبطة بالجريمة الإلكترونية والحرص على تطوير وسائل مكافحتها.
10. استخدام برمجيات آمنة ونظم تشغيل خالية من الثغرات.
11. الحرص على استخدام كلمات سرية للوصول إلى البرامج الموجودة على جهاز الحاسوب.
12. عدم ترك جهاز الحاسوب مفتوحاً.
13. فصل اتصال جهاز الحاسوب بشبكة الإنترنت في حال عدم الاستخدام.
14. أخذ الحيطة والحذر وعدم تصديق كل ما يصل من إعلانات والتأكد من مصداقيتها عن طريق محركات البحث الشهيرة.
15. وضع الرقم السري بشكل مطابق للمواصفات الجيدة التي تصعّب من عملية القرصنة عليه من هذه المواصفات بأن يحتوي على أكثر من ثمانية أحرف أن يكون متنوع الحروف والرموز واللغات إلخ.
16. يفضل تغيير كلمة المرور الخاصة بك بصفة دورية

17. لا تضع معلومات علي الانترنت لا تحب أن يراها الجميع من تعرفهم ولا تعرفهم وتذكر أنه بمجرد أن تضع معلومات علي الانترنت لن تتمكن أبدا من ارجاعها مرة أخرى حتى لو قمت بحذفها
18. معلوماتك الخاصة (اجعلها خاص) ان معلوماتك الخاصة مثل اسمك بالكامل ورقم هاتفك ورقم الهوية ورقم بطاقتك الائتمان وايضا عنوانك بالتفصيل هي معلومات خاصة لا يجب ان تتاح للجميع علي الانترنت لا شخص لا تعرفه فلا تفصح له عنها او تضعها علي اي موقع لا تثق به.

النتائج

من أهم النتائج التي توصل إليها الباحث من خلال هذه الدراسة :

1. نظام المعلومات مصطلح واسع الدلالة يشمل في معناه المكونات المادية لأجهزة الحاسوب أو الشبكات التي تربط بينها كما يشمل البيانات والمعلومات والبرامج وقواعد البيانات والمصنفات الأخرى التي يتم إعدادها بوساطة الحاسوب.
2. يؤيد الباحث ما ذهب إليه الاتجاه الحديث في تحديد مفهوم المال ، بأنه يشمل الأشياء التي تكون لها قيمة اقتصادية، وان المعلومات ليست بمنأى عن هذه القيمة، وأن المعلومة وبالنظر إلى حقيقتها الذاتية واستقلالها تعد قيمة في ذاتها ولها بالتأكيد مظهر معنوي، ولكنها تملك قيمة اقتصادية مؤكدة، وبحيث يمكن عند الاقتضاء أن ترفعها إلى مصاف القيمة القابلة لأن تحاز حيازة غير مشروعة .
3. تعد المعلومات المخزنة في جهاز الحاسوب أموالا مادية منقولة مما يتيح المجال لإمكانية اعتبارها محلا صالحا لجريمة إتلاف الأموال المقررة في قانون العقوبات من حيث المبدأ، إلا أن هذه النصوص التقليدية تبقى قاصرة عن حماية المعلومات في مواجهة العديد من صور الإتلاف المستحدثة للمعلومات مثل إتلاف المعلومات الاسمية .
4. تضمن قانون الاتصالات تجريم إتلاف منظومات الاتصال و يشمل ذلك المعدات المادية المستخدمة في الاتصال كما يشمل البرامج التي تستخدم لأغراض تشغيل هذه المعدات أما ما عداها من معطيات كالرسائل الإلكترونية عبر شبكة الإنترنت أو المعلومات الأخرى المخزنة في أجهزة الحاسوب فلا يشملها نطاق التجريم .
5. يعد الضرر الناجم عن الإتلاف النتيجة الجرمية لهذه الجريمة، وفى الحالة التي يهدف فيها الفاعل إلى إحداث الضرر إلا أن النتيجة الجرمية لا تتحقق لأسباب خارجه عن إرادته كحالة إدخال فيروس إلى نظام الحاسوب واكتشافه قبل إحداث الضرر فإنها تمثل شروعاً معاقبا عليه .

ثانيا. التوصيات:

1- ضرورة تدخل المشرع بالنص على تجريم جريمة الإرهاب الإلكتروني من خلال نصوص خاصة على الرغم من صلاحية المعلومات من حيث المبدأ لأن تكون محلاً لجريمة الإتلاف بمقتضى النصوص التقليدية في قانون العقوبات باعتبارها أموالاً مادية منقولة فإن هناك اعتبارات متعددة تستوجب تدخل المشرع بالنص على تجريم جريمة الإرهاب الإلكتروني من خلال نصوص خاصة تتمثل فيما يلي:

– إن مسألة حماية المعلومات استناداً للنصوص التقليدية التي تجرم إتلاف الأموال محل جدال فقهي واسع مما يقتضي تدخل المشرع لحسم هذا الخلاف بحيث تكون حدود التجريم والعقاب واضحة بصدد هذه المسألة وفقاً لما يقتضيه مبدأ شرعية الجرائم والعقوبات.

– هناك بعض الحالات التي تفتقر فيها المعلومات المذكورة إلى صفة المال كالمعلومات الاسمية ، وهي جديرة بالحماية الجزائية في ضوء أهميتها الخاصة لصاحبها، الأمر الذي يقتضي تدخل المشرع لحماية المعلومات المعالجة آلياً بحد ذاتها من أي إتلاف يصيبها وبصرف النظر عن قيمتها الاقتصادية.

– تجريم إتلاف المعلومات من خلال نصوص خاصة ضرورة تقتضيها خطورة هذه الجرائم حيث إن العقوبات المقررة كجزاء على جريمة الإتلاف لا تتناسب مع خطورة جرائم إتلاف المعلومات مما يقتضي إقرار عقوبات خاصة بها .

2- ضرورة أن تتضمن النصوص القانونية الخاصة بجريمة الإرهاب الإلكتروني توافر حماية لنظام المعلومات بوصفه كياناً قائماً بحد ذاته وذلك بتجريم المساس به بإدخال المعلومات فيه أو محوها أو تعديلها بحيث يشكل هذا السلوك جريمة قائمة بذاتها بدلا من البحث في النتيجة المترتبة على ذلك وبما يغني عن اللجوء إلى النصوص المتناثرة في قوانين العقوبات في إطار جرائم الأموال إذا ترتب على الفعل مساس بحق الملكية أو إطار جريمة التزوير إذا ترتب على الفعل مساس بقيمة المعلومات في الإثبات أو القوانين الخاصة بحماية حق المؤلف إذا ترتب على فعل مساس بالسمعة الأدبية لمؤلف المعلومات أو تعديل في البيانات الاسمية التي تهدف إلى إثبات مؤلف المعلومات في الأحوال التي تمثل فيها هذه المعلومات مصنفاً فكرياً لبرامج الحاسوب المبتكرة.

3- ضرورة أن تتضمن النصوص الخاصة تجريم الدخول غير المصرح به إلى نظام المعلومات دون اشتراط تحقق الضرر نتيجة لذلك مع تشديد العقوبة في حالة وقوع الضرر فعلا .

المراجع:

إبراهيم، مصطفى (1985) **المعجم الوسيط**، ج2،ط3، مجمع اللغة العربية، القاهرة.

إبراهيم، خالد ممدوح (2009). **الجرائم المعلوماتية**، دار الفكر الجامعي، الإسكندرية، ط1.

الجبور، محمد (2012) **الوسيط في قانون العقوبات– القسم العام**، دار وائل للنشر والتوزيع، عمان، ط1

خاطر، نوري حمد (2000) حماية المصنفات والمعلومات ذات العلاقة بالحاسوب بقانون حماية حقوق المؤلف، **مجلة المنارة** العدد (2)، جامعة آل البيت، المفرق.

خالد، حمدي (1992) **الحماية القانونية للكيانات المنطقية (برامج المعلومات)**، أطروحة دكتوراة غير منشورة، جامعة عين شمس

رستم، هشام (1995)، جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة، ورقة عمل مقدمة إلى اللجنة العلمية لإعداد التقرير الوطني المصري لمؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاقبة المجرمين، **مجلة الدراسات القانونية**، جامعة أسيوط، عدد 17، القاهرة.

رمسيس، بهنام (1981)، **النظرية العامة للقانون الجنائي**، منشأة المعارف، الإسكندرية

الزعبي، محمد بلال وآخرون (1999) **الحاسوب والبرمجيات الجاهزة**، ط3، دار وائل للنشر والتوزيع، عمان.

الزعبي، محمد علي (2003) **الحماية القانونية لقواعد البيانات وفقا لقانون حماية حق المؤلف**، ط1، منشأة المعارف، الاسكندري.

السعيد، العشري (2000) **الحاسب الآلي ونظم المعلومات**، ط1، بستان المعرفة، الإسكندرية.

عبابنة، محمد أحمد (2005). **جرائم الحاسوب وأبعادها الدولية**، دار الثقافة، عمان، ط1.

العريمي، مشهور (2009) **الشرعية الدولية لمكافحة الإرهاب**، دار لثقافة للنشر و التوزيع ، عمان.

بهلوان، علي (2010) **استخدام قاعدة البيانات ومنتج التطبيقات**، دار الكتب العلمية للنشر والتوزيع، ط2، القاهرة.

عمار، ماجد (1989) **المسؤولية القانونية الناشئة عن استخدام فيروس برامج الكمبيوتر ووسائل حمايتها**، ط1، دار النهضة العربية، القاهرة.

فكيرين، محمد (1993) **أساسيات الحاسب الآلي**، ط1، دار الراتب الجامعية، بيروت.

فلاح، فادي (2004) **رسالة المعلومات الإلكترونية في القانون الأردني**، رسالة ماجستير غير منشورة، الجامعة الأردنية.

قانون الجرائم الالكترونية الاردني رقم (18) لسنة 2015.

قانون العقوبات الأردني رقم 16 الصادر عام 1960

قانون رقم 46 لسنة 2007 الخاص بمكافحة غسل الأموال و تمويل الإرهاب و تعديلاته

قانون منع الإرهاب الأردني رقم (55) لسنة 2006

القطاونة، مصعب (2010). **الإجراءات الجنائية الخاصة في الجرائم المعلوماتية**، بحث مقدّم لشبكة قانوني الأردن

القهوجي، علي عبد القادر (2000). **الحماية الجنائية للبيانات المعالجة إلكترونياً**، بحث مقدّم إلى مؤتمر القانون والكمبيوتر والإنترنت والذي عُقد خلال الفترة من 1–3 مايو، كلية الشريعة والقانون، جامعة الإمارات العربية.

قورة، نائلة عادل (2012). **جرائم الحاسب الآلي الاقتصادية**، منشورات الحلبي الحقوقية، بيروت، ط1

لطفي، محمد حسام (1994) **عقود خدمات المعلومات**، ط1، بدون ناشر، القاهرة.

مطالقة، محمد فواز (2004) **النظام القانوني لعقود إعداد برامج الحاسوب**، ط1، دار الثقافة، عمان.

العدد الثامن والعشرون
تاريخ الإصدار: 2 – شباط – 2021 م
www.ajsp.net
ISSN: 2663-5798

مطر، عصام عبد الفتاح (2008) **الجريمة الإرهابية**، دار الجامعة الجديدة، الاسكندرية.

المناعسة، أسامة والزعبي ، جلال، والهواوشة ، صايل (2001) **جرائم الحاسب الآلي والانترنت**، دراسة تحليلية مقارنة، دار وائل للنشر، عمان.

نجم، محمد صبحي (1988)، **شرح قانون العقوبات الإربني، القسم العام**، منشورات الجامعة الأردنية، عمان.

اليوسف، عبد العزيز (1999)، **التقنية في الجرائم المستحدثة، بحث ضمن كتاب الظواهر الإجرامية المستحدثة وسبل مواجهتها**، منشورات أكاديمية نايف للعلوم الأمنية ، الرياض

"The Extent of The Adequacy of The Criminal Protection in The Jordanian Legislation to Face The Crimes of Electronic Terrorism"

Preparation:
Tayel Mazen Al-Qadi

Abstract

This study aimed to identify electronic crimes in general and crimes of electronic terrorism in particular, and the position of the Jordanian penal legislator on crimes of electronic terrorism and compare that with some comparative legislation. This study dealt with electronic crimes in general and electronic terrorism crimes in particular with a comparative descriptive analytical approach based on a description The phenomenon of electronic crimes and crimes of electronic terrorism, and one of the most important results that the researcher reached through this study is that the information system is a broad term meaning that includes the physical components of computers or networks that link them as it smells. L Data, information, programs, databases and other works that are prepared by the computer, and the information stored in the computer is considered material material transferred, and the researcher reached many recommendations, the most important of which are: The need for the legislator to interfere with the text to criminalize the crime of electronic terrorism through special texts despite the validity of the information In principle, it should be the subject of the crime of destruction according to the traditional texts in the Penal Code as it is transferred material funds