ELQarar® For Scientific Research | Refereed Journal | Issue 6, Vol 2, Year 1 | June 2024
ISSN 3006-7294

الجريمة الالكترونية كوجه مستحدث من وجوه الجريمة

إعداد

د. زهير خريبط خلف[1]

الملخص

تشكل الجرائم الالكترونية واحدة من أخطر صور الإجرام في العصر الحالي، نظرا لارتباطها الكبير بالتطور التكنولوجي الحاصل على مختلف الأصعدة.

وتعد الجرائم الإلكترونية جريمة ضد أجهزة الكمبيوتر ونظام المعلومات بهدف الحصول على وصول غير مصرح به والتحكم في الجهاز أو حرمان المستخدم أو المالك الشرعي من الوصول إلى النظام. كما قد يتم ارتكابها ضد الأشخاص من خلال الاستعانة بهذه الأجهزة والأنظمة لتشكل جرائم خبيثة شكلت معضلة للدول التي تسعى جاهدة لمكافحتها.

ويعد كلا من جريمتي الاحتيال الالكتروني والذم الالكتروني من الأمثلة البارزة على هذا النوع من الإجرام المستحدث، حيث تعد صور جديدة لجرائم كلاسيكية كانت معروفة مسبقا.

وتتطلب هذه الجريمة كغيرها من أنواع الجرائم، توفر الركنين المادي والمعنوي، مع السعي الدائم للدول من أجل الحفاظ على مبدأ الشرعية من خلال تكريس الركن الشرعي لها عبر تجريم مختلف الأفعال المؤدية لها.

1- استاذ جامعي في كلية شط العرب – البصرة العراق، دكتوراه في القانون العام من الجامعة الاسلامية في لبنان.

المقدمة

كان لحصول التطور التكنولوجي المعاصر وسيطرته على المجتمعات في كافة نواحي الأحياء، آثار إيجابية كثيرة، تمثلت على سبيل المثال وليس الحصر بانتشار في التقنية العالية، من برامج متقدمة[2]، وحسابات آلية، أو الحاسب الآلي[3]، وشبكات اتصال، ساهم في تقريب المسافات بين ملايين من البشر، وخلق فرص جديدة سهلت من عملية الوصول إلى المعلومات، وتبادلها، حتى أصبح يسمى هذا العصر، بعصر المعلومات.

فالكمبيوتر على سبيل المثال الذي زادت أهميته نتيجة التطور التكنولوجي الضخم، في شتى مجالات الحياة المعاصرة، فلم يعد يوجد فرع من أي نشاط إلا ويستخدم في معاملاته الكمبيوتر ومن أكثر الأنشطة التي تستخدم الكمبيوتر البنوك والشركات والهيئات والمطارات وغيرها، بل هناك من يرى بان المجتمعات المعاصرة ستصوت قريبا من خلال جهاز الكمبيوتر مباشرة[4].

ومن ناحية ثانية، وللأسف، فقد أنتج هذا التطور أنواعاً جديدة من الجريمة تسمى الجريمة الإلكترونية cyber crimes، فقد أثر هذا التطور بخلق فرص جديدة للمجرمين، حيث مكنت مجرمي الفضاء الإلكتروني من تصفح الأنترنت وارتكاب جرائم مثل القرصنة، والاحتيال، والتخريب للكمبيوتر، والإتجار بالمخدرات، والتعامل في معلومات العدالة، والمواد الإباحية، دون القبض عليهم أو الكشف عن جرائمهم، فشكلت بالتالي أنماطاً جديدة ومتعددة من الإجرام المستحدث، كان أبطالها لصوص الحاسب الذين يدخلون إلى أنظمة الحاسب وقواعد المعلومات ويسرقونها، أو يعبثون بها، والجرائم التي تخترق الحماية الأمنية في النظم القانونية حيث يتم تجنب العقاب فيها[5].

2- محمد حسام محمود لطفي، الحماية القانونية لبرامج الحاسب الإلكتروني، دار الثقافة للطباعة والنشر، القاهرة، 1987، ص 07.

3- محمد فهمي طلبه وآخرون، الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، موسوعة دلتا كمبيوتر المكتب المصري، القاهرة، مطابع مكتب القاهرة، 1991، ص 108.

4- عبد الكريم الشامي، جرائم الكمبيوتر والإنترنت في التشريع الفلسطيني، ورقة عمل مقدمة للأمانة العامة لمجلس وزراء الداخلية العرب، سبتمبر، 2004.

5- ذياب البداينة، جرائم الحاسب والانترنت، الظواهر الإجرامية المستحدثة وسبل مواجهتها، مركز الدراسات

وقد هدفنا من خلال هذا البحث إلى توضيح مفهوم الجرائم الالكترونية، وتسليط الضوء على أبرز نماذجها، في محاولة منا

كما تتجلى أهمية البحث من خلال ازدياد معدلات الجرائم الالكترونية في السنوات الأخيرة، مما استدعى زيادة الحرص والإجراءات الخاصة بالوقاية منها، للتمكن من مكافحة هذا النوع الخطير من الإجرام.

وفي سياق غوصنا في تفاصيل الجريمة الالكترونية، من اجل إزالة الغموض الملازم لمفهومها وتوضيح بعض صورها، برزت لدينا الإشكالية الرئيسية التالية،

"ما هي الطبيعة الخاصة المنظمة للجريمة الالكترونية؟»

وقد اعتمدنا المنهج الوصفي التحليلي من أجل تحليل القواعد القانونية المنظمة لهذه الجريمة، إضافة إلى إبراز أهم الآراء الفقهية التي تناولتها.

وقد ارتأينا تقسيم البحث إلى بحثين، حيث تطرقنا في المبحث الأول منه للإطار المفاهيمي المنظم للجريمة الالكترونية، بينما عرضنا في المبحث الثاني منه لجريمتي الاحتيال الالكتروني والذم الالكتروني كأحد أبرز صور هذا الإجرام المستحدث.

والبحوث، الرياض، ص 93 – 126.

المبحث الأول: خصوصية الجريمة الالكترونية

بداية يقتضي الإشارة لعدم وجود اتفاق موحد لتعريف الجريمة الالكترونية، بحيث تختلف الاجتهادات لهذه الناحية، ويعود ذلك إلى سببين، هما سرعة التطور التقني والمعلوماتي الحاصل من جهة، وتباين الدور الذي تلعبه هذه التقنية في الجريمة من جهة أخرى.

كما يقتضي الإشارة أيضا إلى الصعوبة التي تعتري عملية تحديد بداية معينة لنشوء الجرائم الإلكترونية، باعتبار أن الحواسيب الإلكترونية كانت موجودة منذ زمن بعيد، ولكن تختلف عما هي عليه الحواسيب الحالية سواء من حيث الشكل أو السرعة والدقة والتطور الحالي الذي يعتبر نتاج لتطور كبير عبر سنوات عدة.

فقد شهدت فترة التسعينيات من القرن العشرين، توازيا مع انتشار الحواسيب والاعتماد عليها في مختلف نواحي الحياة والأعمال اليومية الخاصة والعامة، بدأت الجريمة الإلكترونية في النمو والبروز أكثر فأكثر، حيث سجل ظهور عدة حالات لهذا النوع من الجرائم المتصل بالحواسيب، حيث تعتبر جريمة سرقة بنك مينيسوتا الأمريكي عام 1966، من أفضل الأمثلة على ذلك، باعتبارها أول سرقة الكترونية يكون هدفها بنك[6].

وسوف نقف في هذا المبحث على المقصود بالجريمة الالكترونية، فنبين تعريفها في المطلب الأول، وخصائصها في المطلب الثاني.

المطلب الأول: تعريف الجريمة الالكترونية

لم يتفق الفقهاء على تحديد مصطلح موحد للجريمة الالكترونية، ولكنهم استخدموا العديد من المفردات التي تدل على هذه الجريمة، مثل جريمة تقنية المعلومات[7]، أو جرائم تكنولوجيا

6- الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، إعداد مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة نزوى، سلطنة عمان، مجلس التعاون لدول الخليج العربي، الأمانة العامة، 2016، ص 25.
7- علي عبود جعفر، جرائم تكنولوجيا المعلومات الواقعة على الأشخاص والحكومة، الطبعة الأولى، منشورات زين الحقوقية، بيروت، 2013، ص 75.

المعلومات، أو الجريمة المتعلقة بالحاسب[8]، أو الجريمة الالكترونية، أو الجريمة الواقعة على النظام المعلوماتي[9].

حيث يتمتع النظام المعلوماتي يتمتع بميزة أنه يمكن أن يكون محلا لارتكاب الجريمة من جهة، ويمكن أن يتم استخدامه لارتكاب الجريمة من جهة أخرى، وبذلك يمكن أن تشكل الجريمة المعلوماتية كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي[10].

وقد انقسم الفقهاء في تعريفهم للجريمة الالكترونية إلى ثلاثة اتجاهات، وهو ما سنبينه في الفرع الأول من هذا المطلب، على ان نسلط الضوء على أبرز التعريفات القانونية التي تناولتها في الفرع الثاني.

الفرع الأول: التعريف الفقهي للجريمة الالكترونية

ينظر جانب من الفقهاء في تعريفه للجريمة الالكترونية إلى وسيلة ارتكابها، ويطلق على هؤلاء أصحاب الاتجاه الفني، ويأتي على رأس هؤلاء الفقيه تايدمان الذي عرفها بانها: «كل أشكال السلوك غير المشروع أو الضار بالمجتمع والذي يرتكب باستخدام الحاسب.[11]"

كما عرفت أيضا من قبل أصحاب هذا الاتجاه بأنها نشاط إجرامي تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الجرمي[12].

أما الجانب الثاني من الفقهاء فقد عرف الجريمة الالكترونية استنادا للمعيار الشخصي، والذي يتطلب لقيام الجريمة الالكترونية المام الفاعل بتقنية المعلومات، ويأتي على رأس هؤلاء الفقيه

8- هلالي عبد الله أحمد، التزام الشاهد بالإعلام في جرائم المعلوماتية، دراسة مقارنة، الطبعة الثانية، الحصري للطباعة والكمبيوتر، 2008، ص 13.
9- جلال محمد الزعبي وأحمد محمد المناعسة، جرائم تقنية نظم المعلومات الالكترونية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2010، ص 28 – 30.
10- هشام رستم، قانون العقوبات ومخاطر المعلومات، دار الفكر والقانون، المنصورة، 2007، ص 120.
11- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2005، ص 15.
12- محمد أمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الامارات، أيار 2000، ص 6.

دافيد تومسون، الذي عرف جريمة تقنية المعلومات بانها أي جريمة يكون متطلبا لاقترافها أن يتوافر لدى فاعلها معرفة بتقنية الحاسب[13]، أو هي ذلك النوع من الجرائم الذي يتطلب الماما خاصا بتقنيات الحاسب الآلي، ونظم المعلوماتية لارتكابها أو التحقيق فيها ومقاضاة فاعلها[14].

علما أننا نرى بأن هذا التعريف يضيق من الأشخاص الذين يعتبرون مرتكبي لهذه الجريمة، سيما انه يتطلب إلماما كبيرا بتقنية المعلومات، مع العلم أنه يمكن أن يتم ارتكاب بعضها كما في حالة الذم الالكتروني من دون أن يكون المرتكب على دراية عميقة بعلم الحاسوب.

ويبقى الاتجاه الثالث وهو الاتجاه الموضوعي والذي عرف الجريمة الالكترونية بانها نشاط غير مشروع موجه لنسخ أو تغيير او حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه[15]. كما عرفت بانها مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن ان تكون جديرة بالعقاب، أو هي سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها[16].

الفرع الثاني: التعريف القانوني للجريمة الالكترونية

في ذات توجه الاتجاه الموضوعي، عرفت المنظمة الأوروبية للتعاون الاقتصادي والتنمية الجريمة المعلوماتية من أجل استخدامه كأساس للدراسات التي تجري في هذا المجال منذ العام 1983، وهو بأنها: «كل سلوك غير مشروع او غير أخلاقي أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات أو بنقلها.[17]"

كما عرفها المشرع القطري بأنها الفعل الذي ينطوي على استخدام وسيلة تقنية المعلومات أو

13- David Thomson، current trends in computer crime، computer control quarterly، Vol 9، number 1, 1991، P: 2.

14- سامي علي حامد عياد، الجريمة المعلوماتية وجرائم الانترنت، دار الفكر الجامعي، مصر، 2007، ص 12.

15- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، مرجع سابق، ص 15.

16- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، بحث منشور في مجلة الحقوق للبحوث القانونية والاقتصادية الصادرة عن كلية الحقوق، جامعة الإسكندرية، العدد 24، 1992، ص 270.

17- عادل يحيى، السياسة الجنائية في مواجهة الجريمة المعلوماتية، دار النهضة العربية، القاهرة، 2014، ص 45.

نظام معلوماتي أو الشبكة المعلوماتية، بطريقة غير مشروعة، بما يخالف أحكام القانون[18].

ويتضح لنا من خلال هذا التعريف، ان المشرع القطري عمد إلى تعريف الجريمة الالكترونية بشكل واضح، ولم يترك ذلك للآراء الفقهية، وما يترتب عن هذه الآراء من تعريفات واسعة أو ضيقة. وعلى العموم يمكننا ان نستخلص مما سبق من تعريفات بأن الجريمة الالكترونية هي كل فعل (سلوك إيجابي او سلبي)، مخالف للقانون يقع بواسطة الحاسوب الالكتروني أو ما في حكمه أو

من خلال استخدام شبكة الانترنت، أو قد يكون السلوك موجها لبرامج الحاسوب او بياناته.

المطلب الثاني: خصائص الجريمة الالكترونية

تتشابه الجريمة الالكترونية مع الجريمة العادية، خاصة لناحية ضرورة وجود الجاني والضحية والسلوك الجرمي، لكنها تتميز عن الجريمة العادية من ناحية الوسائل التي يتم استخدامها في ارتكاب الجريمة الالكترونية.

فالجريمة الالكترونية لا تحتاج لوجود الجاني في مكان حدوثها، وتعتمد على التكنولوجيا الحديثة، ووسائل الاتصال الحديثة، وشبكات الانترنت، لذلك فغن بعض هذه الخصائص مرتبط بالجريمة، وبعضها مرتبط بالجاني نفسه.

لذلك سنسلط الضوء على أبرز خصائص الجريمة الالكترونية التي تميزها عن غيرها من أنواع الجرائم من خلال هذا المطلب وفقا لما يلي:

الفرع الأول: الخصائص المرتبطة بالجريمة الالكترونية

تتعدد الخصائص التي تميز الجريمة الالكترونية من هذه الناحية، فهي تقتضي وجود جهاز الكتروني، حيث أنه عادة ما يتم ارتكاب الجريمة الإلكترونية من خلال الاستعانة بجهاز رقمي مثل الحاسوب أو الهاتف الذكي الخ، واستخدامه ضمن ضوابط معينة، وتجري العملية عبر

18- وفقا للمادة الأولى في الفقرة العاشرة منها، في قانون رقم 14 لسنة 2014، الصادر تاريخ 15/9/2014.

الفضاء الافتراضي، تتجلى خطورة الجريمة الإلكترونية في سهولة ارتكابها وتنفيذها وإخفائها في دقائق معدودة، لذلك تعتبر من أخطر جرائم العصر كونها ذات تطور مستمر وأيضًا تعد من الجرائم العابرة للحدود[19].

وهي تعتبر من أبرز أوجه الجريمة المنظمة، حيث إن قدرة الإنترنت على اختصار المسافات، انعكست على طبيعة الأعمال الإجرامية ولم تعد الجريمة محلية بل أصبحت عالمية، والجريمة الالكترونية يرتكبها صاحبها عن بعد وهو يعين عدم التواجد المادي للجرم المعلوماتي في مكان الجريمة، ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز الكمبيوتر وبني النتيجة أي المعطيات. والجريمة الإلكترونية تنتقل من دولة لأخرى[20].

الفرع الثاني: الخصائص المرتبطة بمرتكب الجريمة الالكترونية

يتميز مرتكبو الجريمة المعلوماتية عن غيرهم من مرتكبي الجرائم التقليدية، فسمات مرتكبيها تتشابه مع سمات مرتكبي جرائم أصحاب الياقات البيضاء. وهم يتمتعون بمستوى مهم من المهارة والمعرفة والخبرة بالحاسوب والانترنت.

فالمجرم المعلوماتي يتميز بالذكاء الحاد، سيما أن هذه الجرائم تفترض وجود ذهنية عميقة، ومقدرات عقلية، باعتبار أن المجرم المعلوماتي لا يستخدم العنف أو الاتلاف المادي في ارتكاب جريمته، بل يعتمد على قدراته العقلية ويحقق أهدافه بهدوء[21].

كما أن المجرم في الجريمة الالكترونية هو مجرم عائد للإجرام، وهذا ما يعد من أهم ميزاته، حيث يقوم بتوظيف مهارته في كيفية عمل الحواسيب وكيفية تخزين البيانات والمعلومات

19- أنجليك عبود، الجريمة الالكترونية، مقال منشور على الموقع الالكتروني: www.farmaamaai.org تاريخ الاطلاع: 16/4/2024

20- هشام محمد فريد رستم، القانون والكمبيوتر والأنترنت، بحث مقدم بجامعة دولة الإمارات العربية المتحدة، تاريخ 1 – 3/أيار/2000.

21- نهلا عبد القادر المومني، جرائم المعلوماتية، مرجع سابق، ص 77.

والتحكم في أنظمة الشبكات في الدخول غير المصرح به مرات ومرات[22].

ويعد السبب الأساسي في عودته للإجرام هو سد الثغرات التي ساهمت في التعرف عليهم ومحاكمتهم في المرات السابقة[23].

والمجرم هذا في أغلب الجرائم الالكترونية لا تتجه نيته في ارتكابها إلى تحقيق هدف الاختراق، بل يهدف إلى شعوره بالذكاء والوقة نتيجة ذلك الاختراق.

22- يوسف امير فرج، الجريمة الالكترونية والمعلوماتية والجهود الدولية لمكافحتها، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، 2011، ص 120.

23- غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت، مرجع سابق، ص 14.

المبحث الثاني: الاحتيال الالكتروني والذم الالكتروني

بدأت جريمة الاحتيال الالكتروني بالظهور والانتشار وارتبطت بتكنولوجيا متطورة هي تكنولوجيا الحاسبات الالية والانترنت، مما أسفر عن تمييزها بمجموعة من الحقائق جعلتها تختلف عن غيرها من الجرائم.

ومثلها مثل جريمة الذم الالكتروني التي تشكل اعتداء على شرف واعتبار المجني عليه، ومساسا بمكانته بالمجتمع، وهي من الجرائم الشكلية التي تتحقق بمجرد توافر العلانية والركنين المادي والمعنوي، دون أن تتطلب نتيجة، شانها شأن التحريض على الجرائم[24].

وسوف نتناول في هذا المبحث هاتين الجريمتين في مطلبين، حيث نعرض في المطلب الأول منه لجريمة الاحتيال الالكتروني، ثن نتناول جريمة الذم الالكتروني في المطلب الثاني.

المطلب الأول: جريمة الاحتيال الالكتروني

تحظى دراسة جرائم الاحتيال الإلكتروني بأهمية متزايدة؛ بسبب انتشار التعاملات من خلال الإنترنت، وتزايد التجارة الإلكترونية والمؤسسات المالية والبنوك، وأن نسبة كبيرة من الأفراد والشركات أصبحت تعتمد في حصولها على كثير من السلع والخدمات عن طريق التعاملات الإلكترونية.

الفرع الأول: تعريف الاحتيال الالكتروني

تناول المشرع العراقي جريمة الاحتيال[25]، إذ قضى بما يلي:

"1. يعاقب بالحبس كل من توصل إلى تسليم أو نفل حيازة مال منقول مملوك للغير لنفسه أو إلى شخص آخر وذلك بإحدى الوسائل التالية:

24- سمير عالية، الجرائم الالكترونية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2020، ص 297ز

25- المادة 456 من قانون العقوبات العراقي رقم 111 لسنة 1969

أ- باستعمال طرق احتيالية

ب- باتخاذ اسم كاذب أو صفة غير صحيحة أو تقرير امر كاذب عن واقعه معينه متى كان من شان ذلك خدع المجني عليه وحملة على التسليم

2. يعاقب بالعقوبة ذاتها كل من توصل بإحدى الطرق السابقة إلى حمل آخر على تسليم أو نفل حيازة سند موجه لدين أو تصرف في مال أو إبراء أو على اي سند آخر يمكن استعماله لإثبات حقوق الملكية أو اي حق عيني آخر أو توصل بإحدى الطرق السابقة إلى حمل آخر على توقيع مثل هذا السند أو الغاءه أو اتلافه أو تعديله."

ويعرف الاحتيال الالكتروني بأنه الاستخدام غير المرخص للبيانات من قبل أي شخص غير حامل للبطاقة الأصلية بهدف الحصول على بضائع أو خدمات، وهذا الاستخدام قد يتطلب استخدام بطاقة حقيقية أو لا يتطلب ذلك، ومنذ أن حققت شبكة الانترنت انتشارا عالميا دخلت إليها عمليات الاحتيال والنصب من أبواب مختلفة، وكانت أشكال الاحتيال الأولى في مواقع الانترنت بعدها انتقلت إلى وسائل الدفع الالكترون ي معتمدا على بساطة الناس وعفوية تعاملهم مع سواهم والمبالغ التي يتم الاستيلاء عليها قد تصل إلى مئات ملايين الدولارات وخصوصا عندما يمنح أحدهم رقم حسابه المصرفي لشخص عبر البريد الالكتروني وتنتشر مراكز عمل المحتالين في البلدان التي تنخفض فيها الرقابة على النشاط المعلوماتي وخصوصا في أفريقيا[26].

فالاحتيال يقع اعتداء على حق الملكية سواء المنقولة أو العقارية، وحق الملكية كما هو معروف حق جامع مانع يخول المالك الحق في استعمال واستغلال الشيء في حدود القانون والتصرف فيه[27].

26- محمد محرم محمد علي، جريمة النصب والاحتيال والتجارة الالكترونية، دون دار نشر، القاهرة، ١٩٩٨، ص 80.

27- أنور العمروسي، الملكية وأسباب كسبها، دار محمود للنشر والتوزيع، دون مكان نشر، 1999، ص 4.

والاحتيال أو النصب الالكتروني هو الاستيلاء أو الحيازة على مال الغير بوسيلة يشوبها الخداع ينتج عنها تسلك ذلك المال عن طريق أجهزة الحاسب الآلي. ويقوم مرتكب هذه الجريمة بالاستعانة بالتقنيات الحديثة بهدف التلاعب في البيانات المصرفية ونتائج الميزانيات والمستحقات المالية، فيتم تحويل تلك الأموال خلال وقت قصير لا يتعدى الثواني المعدودة، وهو ما يزيد من آثارها السلبية الخطيرة جدا على الاقتصاد القومي للدول، حيث انها قد تؤدي لإفلاس العملاء والشركات والبنوك الكبرى في الدولة[28].

الفرع الثاني: أركان الاحتيال الالكتروني

إن جريمة الاحتيال الإلكتروني مثل باقي الجرائم تفترض لقيامها اجتماع أركان الجريمة الثلاثة العامة وهي الركن المادي والركن المعنوي والركن الشرعي.

والمشرع العراقي تناول أركان جريمة الاحتيال من خلال نص المادتين ٤٥٦ و٤٥٧ من قانون العقوبات[29].

الفقرة الأولى: الركن المادي في جريمة الاحتيال الالكتروني

الركن المادي في جريمة الاحتيال هو السلوك الجرمي الذي يتم بموجب طرق احتيالية تتمثل في اتخاذ اسم كاذب أو صفة غير صحيحة، والعنصر الثاني للركن المادي هي الشبكة المعلوماتية، بالإضافة الى العنصر الثالث النتيجة الاجرامية والمتمثلة في تسليم المال من قبل المجني عليه الى الجاني، إضافة للركن المعنوي.

وعلى سبيل المثال فيما يتعلق بجريمة الاحتيال عبر شبكة المعلومات الدولية، يتخذ الركن المادي الخاص فيها أشكالا متعددة، منها البريد الإلكتروني الذي تم إرساله أو الأداة الإلكترونية التي يتم الاستعانة بها في ارتكاب جريمة الاحتيال المعلوماتية، أو الأدوات التي تم تصميمها،

28- هدى قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية للنشر والتوزيع، القاهرة، 1992، ص 50 وما يليها.
29- وفقا للمادة ٤٥٦ والمادة ٤٥٧ من قانون العقوبات العراقي، رقم 111 لسنة 1969، المعدل.

أو تم الاستعانة بها من خلال الاتصال أو الإيقاع بالضحية كما يلزم توفر الأداة التي تم إرسال الرسالة من خلالها والتي تتمثل في هذه الحالة الجهاز الحاسوبي لإتمام عملية الاحتيال، أو الوصول إلى قواعد بيانات غير مسموح بالاطلاع عليها، أو استخدامه للوصول إلى معلومات موجودة على جهاز حاسوبي أخر، وكلها أمور كفيلة بأن تثبت توفر الركن المادي للجريمة[30].

الفقرة الثانية: الركن المعنوي في جريمة الاحتيال الالكتروني

أن الركن المعنوي في جريمة الاحتيال الإلكتروني يتطلب علم الجاني بعناصر الجريمة المرتكبة وعلمه ينصب على أن الحاسب الآلي الذي يجري اختراقه أو الحساب الذي يتم الدخول إليه بشكل غير مشروع هو ليس له أو أن المال الذي يستولي عليه هو مال ليس له إنما هو مال مسروق، أو أن البيانات التي قام بالحصول بطريق الاختراق أو القرصنة هو دخول غير مشروع، أو أن الفعل الذي يقوم به هو فعل مجرم, والعلم في جريمة الاحتيال الإلكتروني هو علم مفترض حيث أنه وفقاً للقاعدة القانونية العامة "لا يجوز لأحد أن يعذر بالجهل بأحكام القانون"، كما أنه يجب لحدوث الركن المعنوي أن تتجه إرادة الجاني على إحداث النتيجة الجرمية، وقضت معظم التشريعات الجنائية أن لجريمة الاحتيال الإلكتروني قصد جنائي خاص يتمثل في انصراف نية الجاني المحتال إلى الاستحواذ والاستيلاء على المال محل الجريمة وتملكه ملكية مطلقة[31].

وبمعنى آخر يمكننا القول إنه تعتبر جريمة الاحتيال عبر شبكة المعلومات الدولية جريمة عمدية تقوم على القصد الجنائي العام بركنيه العلم والإرادة، حيث يجب أن تتجه إرادة الجاني إلى فعل الاختراق، أو إلى فعل إعاقة تشغيل النظام، أو إلى فعل الإدخال أو المحو والتعديل، وهذه كلها صور في السلوك الإجرامي في هذه الجريمة، كما يجب أن يعلم بأن نشاطه غير

30- سمير إبراهيم جميل الغزاوي، المسؤولية الجنائية الناشئة عن استخدام الانترنيت، رسالة ماجستير مقدمة الى كلية القانون، جامعة بغداد، ص 98.

31- سامر سلمان عبد الجبوري، جريمة الاحتيال الالكتروني، دراسة مقارنة، رسالة ماجستير، جامعة النهرين، كلية الحقوق، قسم القانون العام، العراق، 2014، ص 27.

مشروع وأنه يعتدي على صاحب الحق في المعطيات، أو من له السيطرة عليها.

المطلب الثاني: جريمة الذم الالكتروني

لقد انتشرت في الآونة الأخيرة، أفعال الذم المرتكبة عبر وسائل التواصل الاجتماعي وسار الجدال حول كيفية مكافحة هذا النوع من الإجرام المستحدث. سيما وأن تجريم الذم لا يهدف لمواجهة شخص المجني عليه، بما يؤلمه ويتأذى به من العبارات المهينة، إنما ما يشين اعتباره وكرامته وتعريضهما للخطر من جراء سماع الكافة عنه هذا الذم. وهذا المبرر يتحقق بمجرد توافر العلانية في الاعلام، ولو لم يعلم المجني عليه بما رمي به.

وسوف نتناول هذا المطلب من خلال الفرعين التاليين، في محاولة منا لتسليط الضوء على جريمة الذم الإلكتروني.

الفرع الأول: تعريف جريمة الذم الالكتروني

يعرف الذم الالكتروني بأنه نسبة أمر إلى شخص بواسطة إحدى وسائل الإعلام المكتوب أو المرئي أو المسموع أو الإلكتروني، ولو كان صادقا لأوجب عقاب من أسند إليه بالعقوبة المقررة لذلك قانونا، أو أوجب احتقاره عند أهل وطنه[32].

وقد عرّفت المادة 385 من قانون العقوبات اللبناني الذم بأنه نسبة أمر الى شخص (ولو في معرض الشك أو الاستفهام) ينال من شرفه أو كرامته.

الفرع الثاني: اركان جريمة الذم الالكتروني

يقتضي لقيام جريمة الذم الالكتروني ركنان: ركن مادي وآخر معنوي.

الفقرة الأولى: الركن المادي

يتمثّل الركن المادي لجريمة الذم بالمظهر الخارجي له، أي في سلوك يصدر عن الجاني. وقد

32- سمير عالية، الجرائم الالكترونية، مرجع سابق، ص298.

اعتبر الاجتهاد أن جرم الذم يتحقّق نتيجة توافر ثلاثة عناصر، هي: وجود واقعة محددة جرى إسنادها الى شخص المجني عليه، وأن يكون من شأن هذا الإسناد المساس بشرف واعتبار ذلك الشخص، وأن يكون قد جرى الإفصاح عنها علناً. ولا بد من أن يكون الفاعل قد نسب في أية صيغة كلامية أو كتابية أمراً محدداً للمجني عليه أو حادثة من شأنها المساس بشرفه واعتباره. فلا يكفي قيامه باستعمال ألفاظ أو تعابير عامة أو إطلاق حكم قيمي على تصرفات المجني عليه.

وتتحقّق جريمة الذم بأية وسيلة من الوسائل المذكورة في المادة 209 عقوبات.

كما تتحقّق جريمة الذم إذا وقع الفعل الجرمي على سبيل اليقين أو الشك أو الاستفهام، صريحاً كان أو ضمنياً، وسواء كان مصدره المعلومات الخاصة أو رواية منقولة عن الغير أم إشاعة يرددها الجاني، على أن يكون من شأن كل ذلك النيل من شرف الشخص أو كرامته.

وهناك بعض الصفات التي يقتضي أن تكون موجودة في الضحية، وهي أن يكون المذموم محدداً تحديداً كافياً لا لبس فيه، ولكن هذا لا يعني وجوب تعيين المذموم باسمه وأوصافه تعييناً دقيقاً، بل يكفي أن تكون عبارات الذم موجهة على صورة يسهل معها فهم المقصود منها ومعرفة الشخص الذي يعنيه الجاني؛ فإذا تمكّنت المحكمة من فحوى عبارات الذم تحديد من هو المعني به من دون تكلّف أو عناء، كانت الجريمة قائمة. وتقوم جريمة الذم إذا ذكر الجاني الأحرف الأولى من اسم المذموم، أو صفة ملازمة له، أو مهنته، أو وضع صورته الى جانب المقال. وتعود لمحكمة الأساس مسألة تقرير ما إذا كان المذموم محدداً أم غير محدد[33].

الفقرة الثانية: الركن المعنوي

تعتبر جريمة الذم بشكل عام من الجرائم القصدية، وبالتالي يجب توافر القصد الجرمي للذم في جميع حالاته، وهو القصد العام الذي يتطلّب وجود علم بعناصر الجريمة وإرادة تتجه الى

33- نادر عبد العزيز شافي، جرائم الذم والقدح وعقوباتها في القانون اللبناني، مجلة الجيش، تموز 2010. منشور على الموقع الالكتروني للجيش اللبناني: lb.gov.lebarmy.www

السلوك المكوّن لها ونتيجته الرامية الى النيل من شرف المذموم وكرامته[34].

ومن البديهي أن تكون جريمة الذم الالكتروني مثل جريمة الذم، باعتبار انها إحدى صورها المستحدثة مع شرط أن يتم ارتكابها بواسطة الحاسوب او ما يماثله ومن خلال استخدام الانترنت.

ويفترض القصد الجرمي عندما تكون العبارات شائنة بذاتها، وهو افتراض يقبل إثبات العكس، فالمتهم يستطيع أن يثبت عدم علمه بأن عبارات الذم شائنة إن كان لها في بيئته معنى غير شائن وهو يجهل دلالتها الشائنة في بيئة المجني عليه[35].

والالزام بوجود نية الضرر هو أمر بديهي في هذه الجريمة، باعتبار أن مرتكبها يهدف للنيل من سمعة وشرف الضحية، كما أن المصلحة التي تكمن وراء تجريمها هو في حماية كرامة وشرف الضحية وسمعته. لأن من يرتكب هذه الجريمة لا يهدف لقتل الضحية أو سرقتها، كما ان هذه الجريمة قد تفتح الباب أمام أنواع أخرى من الجرائم، كالابتزاز والتهديد، حيث قد يعمد المرتكب إلى تهديد الضحية لحثها على القيام بعمل معين او الامتناع عنه مقابل وقف الذم الالكتروني بحقها.

34- محمود نجيب حسني، شرح القسم الخاص المصري، مرجع سابق، رقم 827، ص 549.
35- سمير عالية، الجرائم الالكترونية، مرجع سابق، ص 306 – 307.

الخاتمة

نعيش اليوم في عالم يحكمه التطور التكنولوجي والمعلوماتي، الذي أوجد ظاهرة متعددة الأبعاد ونطاق التأثير والملامح، تشكل تهديدا للدول بدرجة تفوق تهديد الدول لبعضها البعض وهذه الظاهرة الخطيرة ممثلة في الإرهاب الالكتروني، هذا الشكل المتطور للإرهاب العادي يعتمد على استخدام الإمكانات العلمية والتقنية، واستغلال وسائل الاتصال والشبكات المعلوماتية، وهو يمثل وباءاً حقيقيا يصور شتى أنواع العدوان وصور الفساد بصورة متطورة تستفحل العقول وتنشر الرعب والخوف في العالم.

النتائج

اما أبرز النتائج التي توصلنا إليها فهي:

– تشكل الجريمة الالكترونية أحد أبرز وأخطر أنواع الإجرام المستحدث في عصرنا الحديث الذي ينتج عنه آثار خطيرة جدا.

– تعددت التعريفات الفقهية التي تناولت الجريمة الالكترونية، لكن التعريف الأبرز برأينا هو أنها سلوك سلبي أو إيجابي لارتكاب فعل مخالف للقانون باستخدام أدوات الحاسب الآلي أو تقنية المعلومات، أو ضرب برامج أو بيانات محددة (معلومات).

– إن الجرائم الالكترونية كأي جريمة عادية تتطلب لقيامها توفر الركن المادي والمعنوي مع عنصر مفترض هو الحاسب الآلي او ما يماثله وشبكة الانترنت.

– إن الجرائم الإلكترونية باتت تتخذ أنماطا جديدة وضرباً من ضروب الذكاء الإجرامي، وهذا ما يمثل تحديا جدياً وجديداً في الوقت الحاضر.

التوصيات

اما أبرز التوصيات فهي:

– بذل الجهود الدولية في سبيل التعاون وتبادل الخبرات المعلوماتية والعلمية من أجل مكافحة هذا النوع المستحدث من الإجرام.

– نشر الوعي والثقافة في المناهج العلمية والتربوية في المدارس والجامعات، وعبر الأجهزة الأمنية المختصة من اجل الحؤول دون وقوع مزيد ضحايا الجريمة الالكترونية.

– العمل على ابتكار طريقة خاصة للتواصل بين المواطنين والأجهزة الأمنية المعنية، تكون بمثابة خص ساخن، وذلك لتفعيل مشاركتهم في مكافحة جرائم الانترنت، وتحديدا الجرائم الأخلاقية، لا سيما استغلال الأطفال الجنسي، وممارسة الفجور عبر الانترنت.

– تضافر الجهود الدولية من أجل سن القوانين والتشريعات الدولية المستمدة من الظروف العملية والقاضية بمواجهة جرائم الإنترنت، وإلزام كافة دول العالم بتطبيق تلك القوانين لضمان القضاء أو التخفيف من هذه الجرائم على شبكة الإنترنت.

وكخلاصة لما سبق من دراسة لبحثنا، برزت لدينا الإشكالية التالية التي نعتقد بأنها قد تشكل أساسا لدراسات مستقبلية:

"ما هو الدور القانوني الذي يمكن للذكاء الاصطناعي أن يلعبه في مكافحة الجريمة الالكترونية؟»

المراجع

الكتب

• أنور العمروسي، الملكية وأسباب كسبها، دار محمود للنشر والتوزيع، دون مكان نشر، 1999.

• جلال محمد الزعبي وأحمد محمد المناعسة، جرائم تقنية نظم المعلومات الالكترونية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2010.

• ذياب البداينة، جرائم الحاسب والانترنت، الظواهر الإجرامية المستحدثة وسبل مواجهتها، مركز الدراسات والبحوث، الرياض، دون تاريخ نشر.

• سامي علي حامد عياد، الجريمة المعلوماتية وجرائم الانترنت، دار الفكر الجامعي، مصر، 2007.

• سمير عالية، الجرائم الالكترونية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2020.

• علي عبود جعفر، جرائم تكنولوجيا المعلومات الواقعة على الأشخاص والحكومة، الطبعة الأولى، منشورات زين الحقوقية، بيروت، 2013.

• عادل يحيى، السياسة الجنائية في مواجهة الجريمة المعلوماتية، دار النهضة العربية، القاهرة، 2014.

• غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت وجرائم الاحتيال المنظم باستعمال شبكة الانترنت، دار الفكر والقانون، المنصورة، 2017.

• محمد حسام محمود لطفي، الحماية القانونية لبرامج الحاسب الإلكتروني، دار الثقافة للطباعة والنشر، القاهرة، 1987.

• محمد فهمي طلبه وآخرون، الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، موسوعة دلتا كمبيوتر المكتب المصري، القاهرة، مطابع مكتب القاهرة، ١٩٩١.

• محمد محرم محمد علي، جريمة النصب والاحتيال والتجارة الالكترونية، دون دار نشر، القاهرة، ١٩٩٨.

• محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2005.

• نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة، عمان، 2012.

• هدى قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية للنشر والتوزيع، القاهرة، 1992.

• هلالي عبد الله أحمد، التزام الشاهد بالإعلام في جرائم المعلوماتية، دراسة مقارنة، الطبعة الثانية، الحصري للطباعة والكمبيوتر، 2008.

• هشام رستم، قانون العقوبات ومخاطر المعلومات، دار الفكر والقانون، المنصورة، 2007.

• يوسف امير فرج، الجريمة الالكترونية والمعلوماتية والجهود الدولية لمكافحتها، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، 2011.

المراجع الأجنبية

• David Thomson ،current trends in computer crime ،computer control quarterly، Vol 9 ،number 1, 1991 ،P: 2.

القوانين

• قانون العقوبات العراقي، رقم ١١١ لسنة ١٩٦٩، المعدل.

• القانون القطري لمكافحة الجرائم الالكترونية رقم 14 لسنة 2014، الصادر تاريخ 15/9/2014.

• قانون العقوبات اللبناني.

الرسائل الجامعية

• سامر سلمان عبد الجبوري، جريمة الاحتيال الالكتروني، دراسة مقارنة، رسالة ماجستير، جامعة النهرين، كلية الحقوق، قسم القانون العام، العراق، 2014.

• سمير إبراهيم جميل الغزاوي، المسؤولية الجنائية الناشئة عن استخدام الانترنيت، رسالة ماجستير مقدمة الى كلية القانون، جامعة بغداد، دون تاريخ نشر.

المقالات والأبحاث

• أنجليك عبود، الجريمة الالكترونية، مقال منشور على الموقع الالكتروني: www.far-maamaai.org تاريخ الاطلاع: 16/4/2024

• عبد الكريم الشامي، جرائم الكمبيوتر والإنترنت في التشريع الفلسطيني، ورقة عمل مقدمة للأمانة العامة لمجلس وزراء الداخلية العرب، سبتمبر، 2004.

• علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، بحث منشور في مجلة الحقوق للبحوث القانونية والاقتصادية الصادرة عن كلية الحقوق، جامعة الإسكندرية، العدد 24، 1992.

• نادر عبد العزيز شافي، جرائم الذم والقدح وعقوباتها في القانون اللبناني، مجلة الجيش، تموز 2010. منشور على الموقع الالكتروني للجيش اللبناني: lb.gov.lebarmy.www

• الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، إعداد مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة نزوى، سلطنة عمان، مجلس التعاون لدول الخليج العربي، الأمانة العامة، 2016.

• محمد أمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون

والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الامارات، أيار 2000.

• هشام محمد فريد رستم، القانون والكمبيوتر والأنترنت، بحث مقدم بجامعة دولة الإمارات العربية المتحدة، تاريخ 1 – 3/أيار/2000.