جامعة الأزهر
AL-AZHAR UNIVERSITY

ذاتية الجرائم الإلكترونية

إعداد

عبد الهادي حمد محمد بن نورة المري

كلية الدراسات العليا – أكاديمية الشرطة

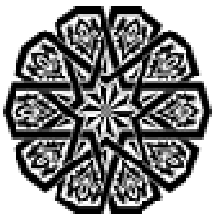
برنامج الماجستير في القانون

بحث مستل من الإصدار الثالث ٢/٢ من العدد الأربعين

يوليو/ سبتمبر ٢٠٢٥م

ذاتية الجرائم الإلكترونية

إعداد



عبد الهادي حمد محمد بن نورة المري

كلية الدراسات العليا – أكاديمية الشرطة

برنامج الماجستير في القانون

موجز عن البحث

يتناول هذا البحث موضوع " ذاتية الجرائم الإلكترونية" ، بوصفها من أبرز الجرائم المستحدثة التي فرضها التطور الهائل في مجالات التقنية والاتصالات والمعلومات، وما نتج عنها من أنماط جديدة من السلوك الإجرامي يصعب ضبطها أو إثباتها وفق القواعد الجنائية التقليدية. فقد أصبحت الجريمة الإلكترونية تمثل تحدياً حقيقياً أمام التشريعات الوطنية والدولية نظراً لخصوصيتها التي تجمع بين الطابع التقني والافتراضي، مما استدعى وضع تنظيم قانوني خاص بها يختلف عن الجرائم العادية في أركانها وأدلتها وطرق مكافحتها.

يسعى البحث إلى تحقيق مجموعة من الأهداف، أبرزها: إبراز خصوصية الجرائم الإلكترونية على المستويين الموضوعي والإجرائي، وبيان أوجه التميز في قواعد التجريم والعقاب مقارنة بالجرائم التقليدية، إضافة إلى توضيح الطبيعة الخاصة لوسائل الإثبات في هذه الجرائم، ودراسة إجراءات التحقيق المتبعة فيها بما يتلاءم مع طبيعتها التقنية. كما يهدف إلى استجلاء موقف المشرع القطري من خلال قانون مكافحة الجرائم الإلكترونية رقم (١٤) لسنة ٢٠١٤، ومقارنته ببعض التشريعات العربية والأجنبية لإبراز مدى فعالية الإطار التشريعي في مواجهة هذه الظاهرة المتنامية.

وقد اعتمد الباحث المنهج الوصفي التحليلي لدراسة النصوص القانونية والأحكام القضائية ذات الصلة، والمنهج المقارن لتحليل تجارب التشريعات المختلفة في معالجة الجريمة الإلكترونية. كما استند إلى مراجع فقهية متخصصة وأبحاث أكاديمية حديثة تناولت أبعاد الجريمة الرقمية من حيث التجريم والعقوبة والإثبات.

وتوصل البحث إلى عدد من النتائج المهمة، من أبرزها أن الجريمة الإلكترونية تتمتع بذاتية خاصة تميزها عن غيرها من الجرائم التقليدية، سواء في بيئتها الرقمية أو في

أركانها القانونية، حيث يتطلب تحققها وجود وسيط تقني أو نظام معلوماتي. كما تبين أن القواعد الإجرائية التقليدية غير كافية لضبط هذا النوع من الجرائم، لأن طبيعة الأدلة الإلكترونية تختلف من حيث الشكل والمضمون، فهي أدلة غير مادية، سريعة الزوال، وقابلة للتعديل أو النسخ، مما يجعل التعامل معها يتطلب خبرة فنية عالية ومعرفة تقنية دقيقة. وأكد البحث كذلك على ضرورة منح سلطات التحقيق صلاحيات أوسع في جمع الأدلة الرقمية وتقديرها بما يتوافق مع مبادئ الشرعية القانونية والحقوق الدستورية للأفراد.

أما التوصيات، فقد تمثلت في ضرورة تطوير التشريعات الوطنية باستمرار لمواكبة التطور التقني المتسارع، وتوسيع نطاق التعاون الدولي في مجال مكافحة الجريمة الإلكترونية عبر تبادل المعلومات وتسليم المجرمين، مع التركيز على تدريب وتأهيل مأموري الضبط القضائي والمحققين والقضاة في مجال تكنولوجيا المعلومات والأدلة الرقمية. كما أوصى البحث بإدراج مواد متخصصة في التحقيق الرقمي والإثبات الإلكتروني ضمن برامج كليات القانون والشرطة لتعزيز القدرات الوطنية في التصدي لهذا النوع من الجرائم.

وبذلك خلص البحث إلى أن مواجهة الجرائم الإلكترونية تتطلب منظومة تشريعية وإجرائية متكاملة تجمع بين الفهم القانوني العميق والتأهيل التقني المتطور لضمان تحقيق العدالة في بيئة رقمية متغيرة.

الكلمات المفتاحية : خصوصية ، الجريمة ، الإلكترونية ، الإثبات ، التحقيق ، التجريم، العقوبة.

The Subjectivity of Cybercrimes

Abdulhadi Hamad Mohammed Bin Noura Al-Marri
Master's Researcher, Department of Law, College of Graduate Studies, Police Academy, Qatar
E-mail: abdulhadialmarri802@gmail.com

Abstract:

This research addresses the topic of "the unique nature of cybercrimes," considered one of the most prominent emerging crimes imposed by the tremendous development in the fields of technology, communications, and information. This development has resulted in new patterns of criminal behavior that are difficult to detect or prove according to traditional criminal law.

Cybercrime has become a real challenge to national and international legislation due to its unique nature, combining technical and virtual aspects. This necessitates the development of a special legal framework that differs from ordinary crimes in its elements, evidence, and methods of combating them.

The research aims to achieve several objectives, most notably: highlighting the unique nature of cybercrimes on both the substantive and procedural levels; demonstrating the distinctive features of the rules of criminalization and punishment compared to traditional crimes; clarifying the specific nature of the means of proof in these crimes; and studying the investigative procedures followed in them in a manner appropriate to their technical nature.

It also aims to clarify the position of the Qatari legislator through the Cybercrime Law No. (14) of 2014 and to compare it with some Arab and foreign legislation to demonstrate the effectiveness of the legislative framework in confronting this growing phenomenon.

The researcher adopted a descriptive-analytical approach to study relevant legal texts and judicial rulings, and a comparative approach to analyze the experiences of different legislations in addressing cybercrime.

The study also relied on specialized jurisprudential references and recent academic research that addressed the dimensions of digital crime in terms of criminalization, punishment, and proof.

The research reached several important conclusions, most notably that cybercrime possesses unique characteristics that distinguish it from other traditional crimes, both in its digital environment and its legal elements, as its commission requires the presence of a technological intermediary or information system.

Furthermore, the research revealed that traditional procedural rules are insufficient for controlling this type of crime because the nature of electronic evidence differs in form and content. It is intangible evidence, ephemeral, and susceptible to modification or copying, making its handling require high-level technical expertise and precise technical knowledge.

The research also emphasized the need to grant investigative authorities broader powers in collecting and evaluating digital evidence in accordance with the principles of legal legitimacy and the constitutional rights of individuals.

The recommendations included the need for continuous development of national legislation to keep pace with rapid technological advancements, and expanding international cooperation in combating cybercrime through information exchange and extradition. Emphasis was placed on training and qualifying law enforcement officers, investigators, and judges in information technology and digital evidence.

The research also recommended incorporating specialized courses in digital investigation and electronic evidence into law and police college curricula to enhance national capabilities in addressing this type of crime.

Thus, the research concluded that confronting cybercrime requires a comprehensive legislative and procedural framework that combines a deep legal understanding with advanced technical training to ensure justice in a dynamic digital environment.

Keywords : Privacy , Crime , Cyber , Evidence , Investigation , Criminalization , Punishment

مقدمة

يشهد العالم منذ بداية ظهور الإنترنت وتطور الوسائل التكنولوجية العديد من الاستحداثات والظواهر والأنشطة المرتبطة بذلك التطور وتلك الوسائل المستحدثة، فنحن الآن نعيش في عالم ما بعد الصناعة وعصر التقنية نتيجة تعاظم الوسائل الإلكترونية وثورة الاتصالات، وما نتج عن ذلك من تحول العالم كله إلى كونية واحدة منفتحة على بعضها وذلك لتطور الوسائل الإلكترونية والإعلامية عما قبل ذلك، إلا أن هذا التطور قد رافقه على الصعيد المقابل تطوراً في ارتكاب الجريمة، بحيث تمخض عن التطور التكنولوجي ولادة ما يعرف **بالجريمة الإلكترونية**، والتي عرفها المشرع الاستخدام غير القانوني لمعدات تكنولوجيا المعلومات أو أنظمة المعلومات أو شبكات المعلومات بشكل مخالف لأحكام القانون[1].

والتي تعتبر أحد الجرائم المستحدثة، والتي تحمل هوية خاصة تختلف عن الجريمة التقليدية في خصائصها باعتبار أن ولادتها تكون في بيئة غير مادية ملموسة تعرف بالبيئة الرقمية، هذه الخصوصية التي سينجر عن حسن فهمها بالضرورة حسن فهم هذا النوع من الجرائم وفهم آلية التعامل معها ومكافحتها، وهو موضوع الدراسة الكامل حول ذاتية الجريمة الإلكترونية.

حيث تعتبر الجرائم الإلكترونية من الأشكال الحديثة للإجرام، نظرا لارتباطها بالتطورات التقنية التي يعرفها العالم، والتي قوامها تكنولوجيا المعلومات والاتصالات، حيث ثبت من خلال أساليب وقوعها وطرق ارتكابها، وتتبع حيثياتها ونتائجها؛ أنها تختلف عن الجرائم التقليدية سواء من حيث نطاقها أو المتضررين منها، أو تقنيات الكشف عنها، مع تسجيل التوظيف السيء للتكنولوجيا في الرفع من احترافية مرتكبي تلك الجرائم، وصعوبة ضبطهم. إنّ دخول المجتمعات إلى عالم الرفاه والسرعة، وتوفر الأدوات المعلوماتية وأجهزة الاتصال قد ساهم في رفع تعداد تلك الجرائم، وتضاعف أعداد ضحاياها، ويمكن تسجيل حقيقة أنها جرائم عابرة للحدود، بحيث لا تقتصر على

ا(١) المادة ١ من القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية.

اقليم دولة واحدة، بل إنها تضم أفرادا وخبرات وأساليب مبتكرة ومستحدثة، تقتضي التفكير بشأن ضبط مفهوم تلك الجرائم، وتحديد مسبباتها، وآليات التعامل القانوني معها.[١]

أهمية البحث:

يكتسي موضوع الدراسة **أهمية نظرية** يُستدل عليها عبر ما أفرزته الجرائم الإلكترونية من جدل قائم حول ما اذا كانت هذه الجرائم ذات خصوصية فعلاً تستوجب اعتناق تشريع خاص للحد من الجريمة المعلوماتية ، فالبعض يرى أن هناك حاجة ملحة لوجود تشريع خاص بالجرائم المعلوماتية يعالج الجانب الموضوعي من جهة والجانب الاجرائي من جهة أخرى، في حين يذهب البعض الآخر الى عدم الحاجة لإفرادها بتشريع خاص وانما الاكتفاء بدمجها مع نصوص في قانون العقوبات التقليدي، إلا أن جل التشريعات الحديثة قد نحت منحى افراد هذا النوع من الجرائم بتشريع خاص اعتباراً لخصوصيتها وما تتمتع به من ذاتية فضلاً عما يترتب عنها من خطورة مبناها طبيعتها الخاصة التي تستوجب الحاجة لقواعد موضوعية واجرائية خاصة في التعامل معها.

وقد انعكست الأهمية سابقة الذكر على **المستوى التطبيقي** بحيث أن انتشار الجريمة المعلوماتية قد أصبح واقعاً متزايداً يوماً بعد الآخر، فضلاً عما يترتب عنها من خطورة لا زالت تتنامى كل يوم عبر ما يتعرض له الافراد من انتهاك للخصوصية أو احتيال أو سب، وهو ما يصعد من أهمية موضوع الدراسة التي تستعى لتسليط الضوء على أحد أبرز وأكثر أنواع الجرائم خطورة في عصرنا الحالي باعتبار ذاتيتها التي تخولها فرصة صعوبة الكشف عن مرتكبها المعروف بالمجرم الإلكتروني.

---

(١) مقلاتي مونة . مشري راضية : الجريمة الإلكترونية: دلالة المفهوم وفعالية المعالجة القانونية، مجلة أبحاث قانونية وسياسية الجزائر،٢٠٢١-٠٦-٠٨.

Volume 6, Numéro 1, Pages 491-510

أهداف البحث:

- إبراز ذاتية الجرائم الإلكترونية على المستوى الموضوعي والمستوى الإجرائي.
- بيان خصوصية عملية الإثبات في الجرائم الإلكترونية.
- بيان خصوصية مرحلة التحقيق في الجرائم الإلكترونية.

إشكالية وتساؤلات البحث:

إن ما سبق كان كفيلاً لضرورة طرح الإشكالية التالية: **ما هي تجليات ذاتية الجرائم الالكترونية في المنظومة التشريعية الجنائية؟**

وللإجابة عن هذه الإشكالية الرئيسية لا بد من الإجابة عن مجموعة من التساؤلات:

١. ما هي تجليات ذاتية الجرائم الإلكترونية على المستوى الموضوعي؟
٢. كيف يمكن إبراز ذاتية الجرائم الالكترونية على مستوى قواعد التجريم؟
٣. كيف يمكن إبراز ذاتية الجرائم الالكترونية على مستوى صور الجرائم؟
٤. ما هي تجليات ذاتية الجرائم الإلكترونية على المستوى الإجرائي؟
٥. هل للجرائم الالكترونية خصوصية في عملية الإثبات ومرحلة التحقيق ؟ وكيف؟

منهجية البحث:

وذلك من خلال أدوات البحث التي تتمثل في مصادر أولية (قانون الجرائم الالكترونية القطري والقوانين المقارنة وفقه القضاء) باستخدام المنهاج الوصفي التحليلي والمنهاج المقارن، مدعوما بمصار ثانوية من (مقالات أكاديمية وكتب ورسائل ماجستير ودكتوراة).

خطة البحث:

وللإجابة عن الإشكالية التي فرضت نفسها فإنه ولإبراز ذاتية هذا النوع من الجرائم فانه يتعين النظر فيها في المنظومة التشريعية الجنائية، ونعني على وجه التحديد تناول ذاتية الجرائم الإلكترونية على مستوى القواعد الجنائية الموضوعية **(المبحث الأول)**، ثم تناول ذاتيتها على مستوى القواعد الإجرائية الجنائية **(المبحث الثاني)**.

المبحث الأول

ذاتية الجرائم الإلكترونية على مستوى القواعد الموضوعية

إن القواعد الموضوعية للجريمة إنما تدور بالأساس حول كل من التجريم والعقاب، وعليه فإن البحث في ذاتية الجريمة المعلوماتية يقتضي النظر في ذاتية هذا النوع من الجرائم وذلك على مستوى قواعد التجريم (**المطلب الأول**) ثم التطرق الى ذاتيها على مستوى قواعد العقاب (**المطلب الثاني**).

المطلب الأول : ذاتية على مستوى قواعد التجريم

تحتاج بعض السلوكيات الإجرامية المستحدثة الى قوالب قانونية جديدة تكون قادرة على تأطيرها، لاسيما إذا كانت القوالب القانونية الجنائية القديمة غير قادرة على استيعابها، بشكل يفرض على المشرع ضرورة التدخل لسن تأطير جديد، وليس أدل على ذلك الجرائم الالكترونية، التي فرضت تدخلاً تشريعياً خاصاً ينظمها، أَبرزَ هذا التشريع الخاص ذاتية الجريمة المعلوماتية على مستوى أركانها من جهة وعلى مستوى صورها من جهة أخرى.

الفرع الأول : أركان الجريمة الإلكترونية

تحتاج الجريمة الإلكترونية كغيرها من الجرائم المعاقب عليها الى جملة من الأركان وهي على النحو التالي:

أولاً: الركن المفترض، هو الشرط الذي يفترض القانون تواجده وقت مباشرة الجاني لفعله وبدونه لا يتصف هذا النشاط بأي جريمة، والشرط المفترض في هذا الإطار يعتبر القاسم المشترك بين الجرائم المعلوماتية، ويتمثل محتواه في استخدام وسيلة تقنية المعلومات أو نطام معلوماتي أو الشبكة المعلوماتية، وبدون ما سبق ذكره لا مجال لوقوع هذه الجريمة.

أكَّد على ذلك **المشرع القطري** صلب القانون رقم (١٤) لسنة ٢٠١٤ المتعلق بإصدار قانون مكافحة الجرائم الإلكترونية حيث تعتبر الجريمة الالكترونية بأنها الاستخدام غير المشروع لمعدات تكنولوجيا المعلومات أو نظم المعلومات أو شبكات المعلومات بما يخالف الأحكام القانونية.[١]

---

(١) المادة ١ من القانون رقم (١٤) لسنة ٢٠١٤ المتعلق بإصدار قانون مكافحة الجرائم الإلكترونية.

ثانيا: الركن الشرعي: وهو ما يعرف بمبدأ شرعية الجرائم والعقوبات، ويفيد مبدأ الشرعية في التجريم والعقاب أن الفعل لا يمكن اعتباره جريمة إلا إذا كان هناك نص قانوني يجرمه،[١] والذي يجد أساسه القانوني في المادة ٤٠ من الدستور الدائم لدولة قطر عام ٢٠٠٤ حيث تنص هذه المادة على أنه " لا جريمة ولا عقوبة إلا بناءً على قانون". وبالنظر في النص التشريعي المنظم للجريمة المعلوماتية يمكن ملاحظة ذاتية الركن الشرعي مقارنة بالنصوص المنظمة للجرائم التقليدية، عبر ما أقره المشرع من اتساع ملحوظ في نطاق التجريم بما يتناسب مع خصوصية هذا النوع من الجرائم.

ثالثاً: الركن المادي: وقد جاء في المادة ٢٦ من قانون العقوبات " يتكون الركن المادي للجريمة من نشاط إجرامي بارتكاب فعل أو امتناع عن فعل، متى كان هذا الفعل أو الامتناع مجرماً قانوناً " والحقيقة أن هذه الصياغة التشريعية للمادة ٢٦ ليست دقيقة نظراً لقصورها على الإلمام بعناصر الركن المادي الذي لا ينحصر في النشاط الإجرامي وإنما أيضاً في النتيجة الإجرامية والعلاقة السببية. وعليه ولفهم ذاتية الركن المادي يتعين التطرق الى العناصر الثلاث للركن المادي في الجريمة المعلوماتية.[٢]

١. **السلوك الاجرامي،** يعرف النشاط الإجرامي بكونه القيام بفعل يأمر القانون تركه أو الامتناع عن القيام بفعل يأمر القانون بفعله، وعليه فإن هذا النشاط الإجرامي يمكن أن يكون إيجابياً أو سلبياً [٣] ، كما ويمكن تعريفه بكونه مخالفة واجب قانوني

---

(١) غنام محمد غنام، بشير سعد زغلول، شرح قانون العقوبات القطري القسم العام – نظرية الجريمة – نظرية الجزاء، إصدارات كلية القانون –جامعة قطر٢٠١٩، ص ١٠.

(٢) من المهم الإشارة إلى أن الجريمة الإلكترونية يمكن أن ترتكب بشكل عمدي أو غير عمدي، فيكون السلوك الإجرامي المكون للركن المادي للجريمة غير مقصود، ومن ذلك على سبيل المثال:

أن يتم تحميل برنامج أو ملفات تحتوي على فيروسات دون علم المستخدم، حيث يمكن أن يؤدي ذلك إلى إلحاق الضرر بأجهزة الكمبيوتر الأخرى عند مشاركة الملفات المصابة عبر الشبكة، وفي هذه الحالة فإن الشخص قد ارتكب جريمة إلكترونية بدون قصد أدت إلى إلحاق نتيجة الضرر بأشخاص آخرين.

للمزيد انظر: الحسن بكار، "الطبيعة القانونية للجريمة المعلوماتية،" مجلة الملف، عدد ١٧ (٢٠١٠).

(٣) غنام محمد غنام، بشير سعد زغلول، شرح قانون العقوبات القطري القسم العام – نظرية الجريمة – نظرية الجزاء، إصدارات كلية القانون –جامعة قطر٢٠١٩، ص ١١٦.

تكفله قوانين العقوبات بنص خاص[١].

وذاتية هذا العنصر في الجريمة الالكترونية أن النشاط أو السلوك المادي فيها يتطلب وجود بيئة رقمية، واتصال بالإنترنت، وفي الجريمة المعلوماتية قد يبدأ السلوك الإجرامي بضغطة زر، أو لمسة على الشاشة، فمثلا يمكن أن يقوم المجرم المعلوماتي ببرمجة فايروس، وإرساله إلى أحدهم مما أدى إلى إحداث ضرر في الجهاز الآخر، فالسلوك الإجرامي يتمثل في إرسال هذا الفايروس في تلك الحالة، أي بضغطة زر (نشاط إيجابي)، ويمكن أن يتحقق الركن المادي من خلال الامتناع عن عمل، ومثال ذلك جريمة التزوير المعلوماتي كالشخص الذي يقوم بتغيير الحقيقة من خلال الترك، كمن عهد اليه كتابة محرر الكتروني وتعمد إغفال بيانات مهمة فيه، فيتم تغيير الحقيقة من خلال امتناعه (نشاط سلبي)[٢].

٢. **النتيجة الاجرامية**: وهي الأثر المترتب عن السلوك الاجرامي[٣]، وتبرز ذاتية هذا الأثر في الجريمة المعلوماتية باعتباره ذي طبيعة غير محددة، لأنه يمس الطبيعة المعلوماتية، فقد يكون أثراً مادياً مثل التلاعب ببيانات ومعلومات قد تؤدي إلى إزهاق أرواح كما في الطائرات والسيارات وغيرها من الأمور الحيوية، وقد يكون معنويا مثل التجسس الإلكتروني، أو الحصول على بيانات خاصة، أو صور خاصة[٤].

٣. **العلاقة السببية**: يجب ان يثبت قيام علاقة السببية بين النشاط الاجرامي والنتيجة الاجرامية فمثلا في جريمة انتهاك الحق في الخصوصية عبر الانترنت، يجب أن يكون هناك دخول على الإنترنت باستخدام حاسوب العامل، والقيام باختراق الخوادم المختلفة في مسارها، وبعد ذلك التعدي على خصوصية موقع ما، فالعلاقة السببية

---

(١) فرج القصير، القانون الجنائي العام، مركز النشر الجامعي، تونس، ٢٠٠٦، ص ٨٤.

(٢) ماجد الزارع، الركن المادي في الجرائم المعلوماتية، مذكرة لنيل شهادة الماجستير، جامعة نايف للعلوم الأمنية، ٢٠١٤، ص٧٧.

(٣) فرج القصير، مرجع سابق، ص٩٤.

(٤) عمر رمضان، فكرة النتيجة في قانون العقوبات، دار الاسراء للنشر والتوزيع، الأردن ١٩٩٨، ص ٤-٨.

تثبت بمجرد ثبوت الضرر على المجني عليه، ونسبته إلى الفاعل الذي قام بالسلوك ومن الجدير ذكره أن القانون عادة لا يضع معيارا لقيام علاقة السببية تاركا ذلك لاجتهاد الفقه والقضاء[١] .

رابعاً: الركن المعنوي: وهو اتجاه إرادة الجاني إلى إحداث النتيجة الجرمية ، وعند الحديث عن الركن المعنوي لا بد من ذكر عنصريه العلم والإرادة، فالعلم يعني علم الجاني بالصفة الإسمية والشخصية للبيانات أو أن يعلم بطبيعة الحاسب الآلي بأنه يقوم بعملية المعالجة الآلية للبيانات، أما الإرادة فهي أن تتجه نية الجاني إلى القيام بالمعالجة الآلية للبيانات بأي صورة كانت مخالفة الإجراءات المعتمدة لإجراء المعالجة الإلكترونية للبيانات أي أن القصد المتطلب لقيام هذا النوع من الجرائم هو القصد العام بحيث لا عبرة بالبواعث التي دفعت الجاني إلى ارتكاب فعله، فسواء كان الباعث هو الإضرار المادي بالشخص أم استغلال هذه البيانات للإساءة لسمعة الشخص[٢]، وهو ما طبقته محكمة التمييز في جريمة سب بإحدى وسائل تقنية المعلومات[٣].

الفرع الثاني : ذاتية على مستوى صور الجرائم

تبرز ذاتية الجرائم الالكترونية في هذا الإطار على مستوى التوسع التشريعي في صور الجرائم الإلكترونية، وقد ارتأينا في هذا الإطار الحديث عن هذه الصور تبعاً للقانون المنظم لها وذلك على النحو التالي ذكره:

١.جرائم التعدي الإلكتروني: يمكن تعريف جرائم التعدي الإلكتروني بأنها كافة صور السلوك غير المشروع، والذي يمثل اعتداء بالضرر أو التهديد به على أمن وحماية

---

(١) ماجد الزارع، مرجع سابق، ص ٣٤.

(٢) محمد علي السالم، الجريمة المعلوماتية، مجلة جامعة بابل، مج١٤ ع ٢، ٢٠١٧، ص ٩٤.

(٣) الحكم الصادر عن محكمة التمييز في الجلسة ١٦-١٠-٢٠١٧، الطعن رقم ٦٠، لسنة ٢٠١٧ محكمة التمييز، المواد الجنائية.

جاء فيه " تطبيقاً للمادة ٨ من قانون مكافحة الجرائم الإلكترونية ٢٠١٤ فإن القصد الجنائي في جريمة القذف والسب باستخدام تقنية المعلومات يتوافر متى كانت العبارات التي وجهها المتهم إلى المجني عليه شائنة بذاتها بغض النظر عن الباعث على توجيهها فمتى كانت الألفاظ دالة بذاتها على معاني السب والقذف وجبت محاسبة قائلها بصرف النظر عن البواعث التي دفعته إليها"

الشبكات المعلوماتية، وشبكة الاتصالات، ونظام التحكم الإلكتروني ونظم المعلومات وعمليات جمع المعلومات، أو ما شابها، والذي يقرر لها المشرع جزاء جنائي أو تدبير احترازي [١]، لقد حدد **المشرع القطري** في قانون مكافحة الجرائم الإلكترونية في الفصل الأول من الباب الثاني جرائم التعدي الإلكتروني، ويظهر من أحكام القانون المذكور أن **جرائم التعدي الإلكتروني تأخذ صوراً متنوعة منها** :

- جريمة الدخول العمدي غير المصرخ به أو غير القانوني [٢]أي الولوج غير المشروع إلى نظام معالجة آلية البيانات ويتحقق الدخول بالوصول إلى المعلومات والبيانات المخزنة في النظام المعلوماتي دون رضا من المسؤول عنه[٣].
- جريمة تجاوز الدخول المصرح به أو البقاء غير المصرح به[٤] يمكن تعريف المقصود بالبقاء غير المصرح به بأنه تواجد الشخص داخل النظام المعلوماتي، دون تصريح من صاحب الإذن في التواجد في النظام في الحالات التي يكون فيها الدخول مشروع أو لكون الدخول غير مجرم[٥].
- جريمة الاعتراض غير القانوني[٦] والتي يقصد بها أي نشاط غير مشروع يهدف إلى الاطلاع على محتويات الاتصال من بيانات ومعلومات تتم داخل نظام حاسب آلي واحد أو أكثر تربطها شبكة اتصالات باستخدام الوسائل الفنية التي تمكنه من ذلك[٧].

---

(١) حازم حسن الجمل، الحماية الجنائية للأمن الإلكتروني، ط١، دار الفكر والقانون، مصر ٢٠١٥، ص ١٢-١٣.

(٢) المادة ٢ من القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية.

(٣) محمد كمال الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية: دراسة مقارنة، دار الفكر والقانون للنشر والتوزيع، مصر٢٠١٥، ص ٥٩.

(٤) المادة ٣ من القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية.

(٥) علياء القحطاني، الحماية الجنائية من جرائم التعدي على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية، مجلة القانون والأعمال، ع ٧٥، ٢٠٢١، ص ٢٨.

(٦) المادة ٤ من القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية.

(٧) محمد كمال الدسوقي، مرجع سابق، ص ٧٠.

٢.**جرائم المحتوى:** وتعرف أيضاً بجرائم النشر الالكتروني وهي من الجرائم المستحدثة التي ارتبطت بتقنية المعلومات وتكنولوجيات الاتصالات، فهي من جرائم الحاسب الآلي (Cyber Crimes) التي تعرف من الناحية الفنية بأنها نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل المقصود، كما تُعرف بأنها سلوك ايجابي أو سلبي يقترف بوسيلة معلوماتية لاعتداء على حق أو مصلحة يحميها القانون[١].

وتعتبر جريمة النشر الإلكتروني جريمة عادية، مثلها مثل جرائم النشر الصحفي، إلا أن ما يميزها هو وسيلة ارتكابها ألا وهو الشبكة المعلوماتية وفي هذا الاطار اعتبرت محكمة التمييز أن " استخدام الجاني برنامج "الواتس أب" الذي يعمل بالإنترنت في إرسال رسائل التهديد للمجني عليه لإرغامه على التنازل عن دعوى التزوير- المتداولة في ذلك الوقت - تتحقق به جريمة التهديد وفقاً للمادة ٩ من قانون ٢٠١٤ "[٢].

٣.**جرائم التزوير والاحتيال الإلكتروني:** وفيما يتعلق بجريمة التزوير فقد وقع تعريف التزوير الإلكتروني بكونه أي تغيير للحقيقة يرد على التوقيع أو المحرر أو الوسيط الإلكتروني، كما وذهب البعض الآخر إلى أنه تغيير الحقيقة في المستندات المعلوماتية وذلك بقصد استعمالها [٣]، ومن ذلك تزوير محرر الكتروني رسمي أو غير رسمي

---

(١) أحمد عبد المجيد الحاج، المسؤولية الجنائية لجرائم النشر الإلكتروني في ضوء قانون مكافحة جرائم تقنية المعلومات الإماراتي، مجلة الفكر الشرطي، مج٢٢ ع ٨٥، الشارقة ٢٠١٣، ص ١٧٣.

(٢) الحكم الصادر عن محكمة التمييز في جلسة ١٦-١٠-٢٠١٧، الطعن رقم ٦٣، لسنة ٢٠١٧ محكمة التمييز، المواد الجنائية.

- انظر في نفس الإطار:

- الحكم الصادر عن محكمة التمييز بجلسة ٠٧-٠١-٢٠١٩، الطعن رقم ١٤٣، لسنة ٢٠١٨ محكمة التمييز، المواد الجنائية. والمتعلق بتجريم نشر أخبار وصور عن الحرمة الخاصة للمجني عليها عن طريق الشبكة المعلوماتية

- الحكم الصادر عن محكمة التمييز بجلسة ٢١ من ديسمبر سنة ٢٠٢٠، الطعن رقم ١٦٣ لسنة ٢٠٢٠، تمييز جنائي تعلقت بسب الجاني للمجني عليها ونشر صوراً لها عبر برنامج التواصل الاجتماعي.

(٣) لمزيد الاطلاع يراجع:

- بندر صياح المطيري، جريمة التزوير الإلكتروني في الكويت، مجلة رماح للبحوث والدراسات، ع ٨٨، ديسمبر ٢٠٢٣، ص ١٢٧ وما بعدها.

- غفران مجامل وسيف المصاروة، جريمة التزوير الإلكتروني في التشريع الأردني: دراسة مقارنة، رسالة ماجستير من جامعة مؤتة، الأردن ٢٠٢٣، ص ٨ وما بعدها.

واستعماله مع العلم بأنه مزور[١].

أما فيما يتعلق بجريمة الاحتيال الإلكتروني فهي بأنه كل فعل أو سلوك متعمد من شخص أو مجموعة من الأشخاص بانتحال هوية الشخص طبيعي او معنوي ويستخدم فيه التقنيات الإلكترونية بهدف تحقيق كسب مادي غير مشروع على الأموال أو السندات وذلك عبر استخدام طرق احتياله او اتخاذ اسم كاذب أو صفه غير صحيحة[٢]، ومن قبيل ذلك انتحال شخصية شخص طبيعي أو حتى معنوي، أو اتخاذ اسم او صفة كاذبة للاستيلاء على مال معين[٣].

٤.**جرائم بطاقة التعامل الإلكتروني:** ويقصد بها جملة الأفعال غير المشروعة المتعلقة ببطاقة التعامل الإلكتروني، وقد تتمثل هذه الأفعال في الاستخدام أو الحصول أو تسهيل الحصول دون وجه حق على أرقام أو بيانات بطاقة تعامل إلكتروني عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، وكذلك تزوير بطاقة تعامل إلكتروني بأي وسيلة كانت، فضلا عن صنع أو حيازة أجهزة أو مواد تستخدم في إصدار أو تزوير بطاقات التعامل الإلكتروني، وأخيراً قَبول بطاقات تعامل إلكتروني غير سارية أو مزورة أو مسروقة مع علمه بذلك[٤].

المطلب الثاني : ذاتية على مستوى قواعد العقاب

تعتمد العقوبة في هذا النوع من الجرائم على النتيجة الاجرامية المترتبة عن السلوك الإجرامي الإلكتروني، ومدى خطورة الخطورة المترتبة عن الجريمة المعلوماتية، وفي نطاق الحديث عن العقوبة سنتطرق الى ذاتيتها وذلك على مستوى نوعيها سواء فيما يتعلق بالعقوبات الأصلية (**الفرع الأول**) او فيما يتعلق بالعقوبات التكميلية (**الفرع الثاني**).

---

(١) المادة ١٠ من القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية.

(٢)حمد السليطي، تجريم الاحتيال الإلكتروني في القانون المقارن والقطري، مذكرة لنيل شهادة الماجستير، كلية القانون جامعة قطر، قطر ٢٠١٨، ص ١١.

(٣) المادة ١١ من القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية.

(٤) المادة ١٢ من القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية.

الفرع الأول : العقوبات الأصلية

تعرف العقوبات الأصلية بكونها العقوبات التي تحكم بها المحكمة فقط كجزاء للجريمة، ومن خلال استقراء جملة النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية نلاحظ تدرجاً متعلقاً بالعقوبات الأصلية، وهذا الأخير انما يعكس الخطورة الاجرامية لهذا النوع من الجرائم، وتبرز ذاتية النظام العقابي لهذا النوع من الجرائم في منح المشرع للقاضي سلطة تقديرية واسعة في تقديره للعقوبة.

ونستعرض فيما يلي جملة العقوبات الاصلية المرصودة للجرائم المعلوماتية تبعاً لصور الجرائم المنصوص عليها في القانون رقم ١٤ لسنة ٢٠١٤ المتعلق بإصدار قانون مكافحة الجرائم الالكترونية.

الحبس و/أو الغرامة.

بتصفح هاتين العقوبتين نلاحظ ان المشرع قد رصدهما معاً أو الاختيار بين احداهما في صورة ارتكاب الجرائم الإلكترونية وذلك بصورة متدرجة بحيث يمكن ان تكون العقوبة تتمثل **بالحبس لمدة لا تتجاوز ٣ سنوات وبالغرامة التي لا تزيد عن ٥٠٠ ألف ريال** في كل من جرائم التعدي الإلكتروني[١] وجرائم المحتوى[٢] وأخيراً جرائم التعدي على حقوق الملكية الفكرية[٣].

وأحياناً تكون العقوبة يعاقب بالحبس مدة لا تجاوز سنتين، وبالغرامة التي لا تزيد على (١٠٠,٠٠٠) مائة ألف ريال كما هو الحال في جرائم التعدي الإلكتروني[٤] ، أو بالحبس مدة لا تجاوز خمس سنوات، وبالغرامة التي لا تزيد على (٥٠٠,٠٠٠)

---

(١) انظر ما يلي:

- الفقرة ١ من المادة ٢ من القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية.
- المادة ٣ من القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية.

(٢) انظر ما يلي:

- المادة ٥ من القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية.
- الفقرة ١ من المادة ٦ من القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية.

(٣) المادة ١٣ من القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية.

(٤) المادة ٤ من القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية.

خمسمائة ألف ريال كما في جرائم المحتوى[١] ، وكذلك بالحبس مدة لا تجاوز سنة وبالغرامة التي لا تزيد على (٢٥٠,٠٠٠) مائتين وخمسين ألف ريال في بعض جرائم المحتوى[٢] ، أو بالحبس مدة لا تجاوز عشر سنوات وبالغرامة التي لا تزيد على (٢٠٠,٠٠٠) مائتي ألف ريال أو بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (١٠٠,٠٠٠) مائة ألف ريال في جرائم التزوير والاجتيال الالكتروني[٣].

الفرع الثاني : العقوبات التكميلية

ترتب عن التنامي الملحوظ في انتشار الجرائم الإلكترونية، والتي بدروها أثرت بطريقة خطيرة على المجتمع ضرورة الحاجة لسن عقوبات تتناسب مع طبيعة هذا النوع من الجرائم، بحيث أصبح يتعين أن تكون مرنة تتناسب مع هدف المشرع من سنه لقانون مكافحة الجرائم الإلكترونية[٤]، الامر الذي حذا بمجموعة من التشريعات نحو التوجه لتسليط عقوبة تكميلية تتمثل في المصادرة والتي تعرف بكونها جملة من الإجراءات الوقائية التي تقرر لحماية المجتمع من وقوع الجرائم وايقاع الشر بأفراده وهي تتخذ للوقاية والاحتراز[٥]، كما عرفها البعض بكونها " نزع مال تم ضبطه جبراً من صاحبه لكي يؤول الى الدولة[٦]، وهي من العقوبات التكميلية التي نص عليها قانون العقوبات القطري[٧].

---

(١) المادة ٧ من القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية.

(٢) الفقرة الثانية من المادة ٧ من القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية.

(٣)انظر

- المادة ١٠ من القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية.

-المادة ١١ من القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية.

(٤) الفايز عبد العزيز، العقوبات التكميلية للجرائم المعلوماتية في النظام السعودي، مرجع سابق، ص ٢.

(٥) محمد علي السالم الحلبي، شرح قانون العقوبات، دار الثقافة للنشر والتوزيع، ص ٤٩٩.

(٦) غنام، ص ٣٩٩.

(٧) المادة ٦٥ من القانون رقم (١١) لسنة ٢٠٠٤ المتعلق بإصدار قانون العقوبات.

• العقوبات التبعية والتكميلية هي:

١- الحرمان من كل أو بعض الحقوق والمزايا المنصوص عليها في المادة (٦٦) من هذا القانون.

٢- الحرمان من مزاولة المهنة. ٣- العزل من الوظائف العامة ٤- إغلاق المكان أو المحل العام

٥- الوضع تحت مراقبة الشرطة ٦- المصادرة. ٧- إبعاد الأجنبي عن البلاد.".

نجد أن **المشرع الفرنسي** أبدع في فرض عقوبات تكميلية تماشيا مع السياسة الجنائية الحديثة، حيث فرض في **المادة ٣٢٣-٦** من قانون العقوبات الفرنسي على الأشخاص الطبيعيين المذنبين في هذه الجرائم حظر لمدة خمس سنوات على الأكثر من الحقوق المدنية والأسرية، إضافة إلى حظر لمدة خمس سنوات على ممارسة الوظيفة العامة أو النشاط المهني أو الاجتماعي الذي ارتكبت خلاله الجريمة أو التي ارتكبت فيها، وهذا النوع من العقوبات التكميلية لم نجده في التشريع القطري أو المصري، وذلك رغم مواكبة هذا النوع من العقوبات التكميلية للسياسة الجنائية الحديثة.

وبالعودة **للقانون القطري** نلاحظ انه تضمن الإشارة فقط الى المصادرة في بعض نصوصه [١]، كل ذلك في إقرار منه لذاتية هذا النوع من الجرائم على المستوى العقابي، بحيث ان العقوبة لابد ان تتلاءم والشخص المدان وقدراته وامكانياته والأدوات التي يستعملها في سلوكه الاجرامي.

(١) انظر في هذا الإطار كل من المواد: ٢٦، ٣٥، ٣٦. من القانون المذكور.

المبحث الثاني

ذاتية الجرائم الإلكترونية على مستوى القواعد الإجرائية

يتعين الإشارة في هذا الاطار الى أن الخصوصية على المستوى الإجرائي تبرز في قصور القواعد الإجرائية التقليدية على تأطير هذا النوع من الجرائم، بحيث أن القواعد الإجرائية التقليدية من شأنها عرقلة عمل أجهزة العدالة وسير الدعوى في جميع مراحلها، من أجل ذلك يتعين التطرق لذاتية هذا النوع من الجرائم عبر النصوص الإجرائية في مرحلة الإثبات من جهة (**المطلب الأول**) والتي ستكشف عن صعوبة هذا النوع من الجرائم والتي تتطلب الإلمام العلمي والتكنولوجي، ثم سيقع التطرق للمستوى الثاني من هذه الذاتية الإجرائية لاسيما على مستوى التحقيق(**المطلب الثاني**).

المطلب الأول : ذاتية على مستوى الأدلة

تبرز صعوبة تتعلق بالحصول على الأدلة المعلوماتية وذلك راجع بالأساس للطبيعة الخاصة للجريمة الإلكترونية والوسائل التي يقع استعمالها لارتكاب مثل هذا النوع من الجرائم، فضلاً عن الإمكانية السريعة في محو الأدلة، وفي هذا الإطار يمكن تعريف الدليل الإلكتروني بكونه الدليل المستمد من وسائط ترتبط بتقنية المعلومات وكلها تدور حول استخدام الحاسب الآلي وتطبيقاته وشبكة الإنترنت وغيرها من التقنيات الحديثة، ويتعلق الدليل المعلوماتي بالجريمة المعلوماتية[١].

تعددت تعريفات **الدليل الإلكتروني**، حيث يمكن تعريفه بكونه: بيانات يمكن إعدادها وتراسلها وتخزينها رقمياً بحيث تمكن الحاسب الآلي من تأدية مهمة ما،[٢] كما عُرف بأنه: الأدلة التي يتم جمعها بواسطة الحاسوب في شكل مجالات ونبضات

---

(١) عبد الفتاح حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة ٢٠٠٧، ص ٧٠٩.

(٢) انظر:

- Digital Evidence: information of probative values stored or transmitted in digital form". Mark M. Pollit, Report on Digital Evidence, presented to 13th Interpol Forensic Science Symposium. Lyon, France, Oct 162001, 19. P5.

مغناطيسية وكهربائية يمكن جمعها وتحليلها لاستخدامها من قبل وكالات إنفاذ القانون باستخدام تطبيقات وتقنيات البرمجيات والمكونات الرقمية التي تقدم المعلومات في أشكال مختلفة، بما في ذلك النصوص، والصور، والصوت، والرسومات.[١]

وهو ما يتماشى مع ملامح مفهوم الدليل الإلكتروني التي تناولها المشرع القطري في نطاق تنظيمه للدليل الإلكتروني بحيث نصت المادة رقم ١٥ من قانون مكافحة الجرائم الإلكترونية على أنه "لا يجوز استبعاد أي دليل ناتج عن وسيلة من وسائل تقنية المعلومات، أو أنظمة المعلومات، أو شبكات المعلومات، أو المواقع الإلكترونية، أو البيانات والمعلومات الإلكترونية بسبب طبيعة ذلك الدليل".[٢] يتضح من ذلك أن كل مصادر الدليل الإلكتروني الواقع ذكرها من المشرع القطري تشير الى الطبيعة الخاصة لهذا الدليل والمتمثلة في تواجده في بيئة افتراضية غير مادية.

الفرع الأول : الطبيعة الخاصة للدليل الإلكتروني

يعتمد السلوك الإجرامي المكون للجريمة الإلكترونية على التشفير والتخزين الإلكتروني والأرقام السرية، ما ينجم عنه صعوبة ترك مرتكب السلوك الإجرامي آثاراً مادية يستدل من خلالها على المجرم كما هو الحال في الجريمة التقليدية، فالأدلة في هذا الإطار تكون غير مرئية في بعض الأحيان، ما يترتب عن ذلك صعوبة في تطبيق قواعد الاثبات التقليدية على المعلومات غير المادية[٣].

يستنتج مما سبق عرضه أن الدليل الإلكتروني يمتاز بخصائص وهي أنه

- **أولاً: دليل علمي:** فهو دليل غير ملموس يتكون من بيانات ومعلومات على هيئة إلكترونية[٤].
- **ثانياً: فهو دليل تقني،** استناداً للمصدر الذي جاء منه وهو البيئة الرقمية

---

(١) طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس ٢٠٠٩، ص ٢.

(٢) المادة ١٥ من القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية.

(٣) إبراهيم طه، شرح قانون جرائم المعلوماتية في القانون السوداني لسنة ٢٠٠٧: دراسة مقارنة، مطابع السودان ٢٠٠٨، ص ٦٠-٦١.

(٤) عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية، ص ٦٠-٦١.

أو التقنية، ولدليل الإلكتروني التقني ليس كالأدلة الجنائية التقليدية الأخرى، فالتقنية لا تنتج أدلة مادية ملموسة كالبصمات، إنما تنتج موجات رقمية ذات فائقة السرعة تنتقل بين أجزاء أنظمة التقنية وشبكات المعلومات متعدية حدود المكان والزمان الواحد.[١]

- **ثالثاً: هو دليل متطور ومتنوع**، يؤكد ذلك استعمال **المشرع القطري** في المادة ١٥ عبارة " أي دليل " بحيث أن مصطلح الدليل الإلكتروني يشمل كافة أنواع وأشكال البيانات الرقمية والتي من الممكن تداولها، تقنياً بين وسائل تقنية المعلومات ومن ذلك تتضح خاصية أن الدليل الإلكتروني هو دليل متنوع فقد يتمثل بالبيانات أو الصور او الأصوات السمعية او حتى النصوص المكتوبة [٢]، أما كونه متطوراً فهي تفيد أنها تستخدم في جرائم مستحدثة، فجريمة النصب مثلاً يمكن ارتكابها بالطرق التقليدية التي تنتج أدلة مادية، وكذلك أصبح مع التقدم التكنولوجي من الممكن ارتكابها باستخدام التقنية ما يستدعي مواكبة السلطات المختصة للتطور التكنولوجي.[٣]

وما يؤكد ذاتية هذا النوع من الجرائم ان هذا الدليل فيها يسهل التخلص منه مقارنة مع الدليل في الجريمة التقليدية التي قد تستعمل فيها الأوراق والسلاح والأموال المزورة التي يصعب التخلص منها، كما تبرز الذاتية لهذه الجرائم على مستوى الأدلة في ان هذه الأخيرة قابلة للنسخ ، بحيث ان الدليل الالكتروني يمكن نسخه وتكون لهذه النسخة نفس القيمة للأصل خلافاً للأدلة التقليدية[٤].

---

(١) المرجع السابق، ص ٦٢.

(٢) أسامة العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الأمنية والتدريب م٢٩ ع ٥٨، السعودية ٢٠١٣، ص ٥٨.

(٣) حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، ط١، دار النهضة العربية، القاهرة ٢٠١٧، ص١٩-٢٠.

(٤) عائشة بن قارة مصطفى، مرجع سابق، ص ٦٤.

أما المشرع المصري فقد بين حجية الدليل الإلكتروني في المادة ١١ والتي أكد فيها المشرع على القيمة الفنية للدليل الجنائي الإلكتروني في الإثبات الجنائي عندما تتوافر فيه الشروط الموضحة في القانون.[١] إن هذه الطبيعة الخاصة للدليل الإلكتروني قد انعكست بدورها على نظامه القانوني لاسيما فيما يتعلق بالشروط الواجب توافرها للأخذ به فضلاً عن أنواعه وهو ما سيق تناوله في الفرع الموالي.

الفرع الثاني : نظام الدليل الإلكتروني

يتطلب هذا النوع من الأدلة ضرورة توافر جملة من الشروط التي يتعين الإحاطة بها وهي تتمثل أساساً في ضرورة أن يقع الحصول عليه بطرق مشروعة، كما أنه يتعين ان تكون الأدلة يقينية غير قابلة للشك فيها أي ان تقترب من الحقيقة قدر المستطاع، وعليه فان جملة المخرجات الالكترونية تخضع لتقدير المحكمة.

كما يتعين ان تكون هذه الأدلة قد تمت مناقشتها في المحاكمة الجنائية، بحيث يتعين ان يقع مناقشة الدليل الإلكتروني حتى يصل القاضي الى تكوين قناعة بخصوص قيمة الدليل في الاثبات وفي هذا الإطار ينص **قانون الاجراءات الفرنسي** في فقرته الثانية من المادة ٤٢٧ على أنه " لا يجوز للقاضي أن يؤسس حكماً الا على أدلة طرحت عليه أثناء المحاكمة ونوقشت أمامه في مواجهة الأطراف".

وبعد استعراض ما سبق يتضح مما لا يدع مجالاً للشك أن الدليل المستعمل في نطاق هذا النوع من الجرائم إنما هو ذو طبيعة خاصة ما يبرز ذاتية الجريمة الالكترونية إجرائياً على مستوى الإثبات، بل وتفرض ضرورة توافر أشخاصاُ مختصين في أنظمة البرمجة والحاسوب حتى يتمكنوا من التعامل مع هذه الأدلة بشكل يعمدوا فيه لتفريغ البيانات والمعلومات المطلوبة والواقع البحث عنها من غير اتلافها.[٢]

---

(١) قانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات.

(٢) عبد الله القحطاني، تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية: دراسة تطبيقية على المحققين في هيئة الادعاء العام في مدينة الرياض، رسالة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير في قسم العلوم الشرطية، الرياض ٢٠١٤، ص ٧٢.

المطلب الثاني : ذاتية على مستوى إجراءات التحقيق

تعتبر إجراءات التحقيق الجنائي العامة هي الأساس في التحقيق بالجرائم الإلكترونية، على أنها تتميز ببعض الخصوصية، وإجراءات التحقيق هي جملة الإجراءات التي يقع مباشرتها من قبل السلطة المختصة لهدف البحث عن الأدلة وتقديرها لإثبات حدوث الجريمة ونسبتها الى المتهم[١] ، وتنقسم إجراءات التحقيق الى قسمين منها ما يتعلق بالتحقيق الابتدائي من جهة (**الفرع الأول**) ومنها ما يتعلق بمرحلة المحاكمة من جهة أخرى (**الفرع الثاني**).

الفرع الأول : ذاتية إجراءات التحقيق الابتدائي في الجرائم الإلكترونية

رسم **المشرع القطري** الإجراءات المتعلقة بالجريمة إلا أن الحديث عن الجريمة الإلكترونية هو بالأساس حديث عن بيانات معالجة إلكترونياً وكيانات معنوية، تستوجب إجراءات خاصة، لكنه لم يفصل بشكل كبير فيها، وإنما ذكر بعض الإجراءات ومن ثم فإن سكوته يعتبر إحالة ضمنية إلى قانون الإجراءات الجنائية، وذلك على خلاف **المشرع المصري** الذي فصل في هذه الإجراءات نجده قد فصل في الإجراءات في قانون مكافحة جرائم تقنية المعلومات، فنجده في المادة ٥ تحدث عن منح صفة الضبطية القضائية، ومن ثم في المواد ٦ و ٧ و ٩ فصل في الإجراءات والقرارات المؤقتة، كما نجده تحدث في المادة ٨ عن آليات التظلم من القرارات الصادرة في شأن طلبات حجب المواقع، وفي المادة ١٠ تحدث عن قيد الخبراء في تقنية المعلومات، حيث تظهر أهمية هذه المادة كون الخبراء هم الذين سيستعين بهم القاضي حصرا للتأكد من الدليل الإلكتروني نظرا لخبرة القاضي المحدودة في هذا المجال.[٢]

أما **المشرع الفرنسي** فلم يضع إجراءات خاصة بالجرائم الإلكترونية كون هذه الجرائم جاءت في قانون العقوبات وبالتالي فهي تخضع للإجراءات الجنائية العامة، لكن

---

(١) المرجع السابق.

(٢) انظر المواد من ٥ الى١٠ من قانون رقم ١٧٥ لسنة ٢٠١٨ المتعلق بمكافحة جرائم تقنية المعلومات في جمهورية مصر العربية.

تجدر الإشارة الى ان خصوصية الجرائم الإلكترونية تتطلب إجراءات خاصة تتناسب مع طبيعة هذه الجرائم وذلك ليحقق قانون مكافحة الجرائم الإلكترونية هدفه في محاربة هذا النوع من الجرائم والذي يختلف كما أوضحنا عن الجرائم التقليدية حيث سيقع التطرق لها على النحول التالي:

١.**الانتقال والمعاينة**: يعرف الانتقال بكونه توجه المحقق لمكان الجريمة قصد تكوين فكرة عن الحادث[١]، خلافاً للمعاينة التي تتمثل في ملاحظة الآثار المادية التي خلّفها السلوك الإجرامي[٢] .

وتبرز خصوصية الجريمة الإلكترونية في أن أهمية المعاينة تتضاءل نظراً لأن هذا النوع من الجرائم لا يخلف اثاراً مادية، ولتعويض هذه الأهمية للمعاينة فإنه لابد من تأمين الأجهزة والمعدات التي ستتسلط عليها المعاينة[٣]، كل ذلك من شأنه جعل المعاينة ناجعة في إطار التنقيب عن الجريمة الإلكترونية.

٢.**ندب الخبرة والشهادة**، وهو الإجراء الذي يقع اللجوء اليه إذا اقتضى الامر كشف دليل أو تعزيز أدلة قائمة، وهي استشارة فنية في المسائل التي لا تتوافر لدى أعضاء السلطة القضائية[٤] ، فأصحاب الخبرة الفنية في الميدان المعلوماتي يقع الاستعانة بهم في هذا الإطار من قبل سلطات التحقيق والشرطة، نظراً لما يمتلكونه من الإلمام

---

(١) عبد الرحمن الدهلاوي، الانتقال والمعاينة في نظم دول مجلس التعاون الخليجي، مذكرة لنيل شهادة الماجستير في العدالة الجنائية، جامعة الإمام محمد بن سعود الإسلامية، السعودية ٢٠٠٨، ص ٧.

(٢) علي عدنان الفيل، إجراء التحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، الإسكندرية ٢٠١٢، ص٢٠.

(٣) المرجع السابق، ص ٢١،٢٣.

(٤) انظر:

-الفقرة الثانية من المادة ٣٤ من قانون الإجراءات الجنائية " ولمأموري الضبط القضائي أن يستعينوا بأهل الخبرة، وأن يطلبوا رأيهم شفاهة أو كتابة، ولا يجوز لهم تحليف الشهود أو الخبراء اليمين إلا إذا خيف ألا يستطاع ذلك فيما بعد".

-عبد الحليم بن باردة، إجراءات البحث والتحري عن الجريمة المعلوماتية، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور بالجلفة، الجزائر ٢٠١٥، ص ٨٢.

بالحاسوب والقدرة على التعامل معه دون تعطيل الأدلة او اتلافها، ويتعين على المحقق في هذا الإطار أن يحدد للخبير الدور المطلوب منه على وجه التحديد[١].

٣.**التفتيش**، يهدف الى البحث عن الأدلة وهو يتطلب بالضرورة أمراً قضائياً لمباشرته، ولاعتباره اجراءً خطيراً فقد ضبطه المشرع بقواعد موضوعية وأخرى شكلية.

وفيما يتعلق بضوابطه الموضوعية فسبب التفتيش هو أن تكون بصدد جريمة معلوماتية مع وجود أجهزة تفيد في الكشف عن الحقيقة أما محل التفتيش فهو جهاز الحاسب الآلي بمكوناته وشبكات الاتصال الخاصة به، وقد يكون الشخص محلاً للتفتيش بوصفه من مستخدمي أو مشغلي الحاسب الآلي أو خبراء البرامج وكذا المنازل كمحل الإقامة او المأوى او أي مكان يوجد فيه أي من مكونات الحاسب الآلي حسبما نص قانون الجرائم الإلكترونية.

وعليه ومن الملاحظ من جملة الإجراءات سابقة الذكر أنها وإن كانت الإجراءات نفسها في الجرائم التقليدية إلا أنه في صورة ما إذا تعلق الأمر بجريمة إلكترونية فإن هذه الإجراءات تأخذ نوعاً من الذاتية أي الخصوصية التي تتلاءم وطبيعة الجريمة، كل ذلك بشكل يعطي هذه الإجراءات نجاعة أكبر في البحث عن هذا النوع من الجرائم والقبض على مرتكبيها.

الفرع الثاني : ذاتية إجراءات التحقيق النهائي في الجرائم الإلكترونية:

ترتكز ذاتية الجرائم الالكترونية على مستويين يتمثل الأول في قواعد الاختصاص القضائي المتعلقة بالجرائم المعلوماتية، والثاني حول مظاهر التعاون الدولي في مكافحة هذا النوع من الجرائم.

وفيما يتعلق بقواعد الاختصاص القضائي في الجرائم الإلكترونية، فإن هذه الأخيرة إنما يقصد بها السلطة التي يقررها القانون للقضاء بالنظر في دعاوى معينة يحددها المشرع وفق اجراءات محددة قانوناً، ويكون القاضي مطالباً أولاً بالبت في مسألة

(١) محمد عمري، الإثبات الجزائي الإلكتروني في الجرائم المعلوماتية، مجلة العلوم القانونية والسياسية، مج ١٢ ع ٢، العراق ٢٠١٦، ص ٣١١ وما بعدها.

الاختصاص الدولي، أي في مدى اختصاص القضاء الوطني في الجريمة من عدمه، ثم البحث في الاختصاص الداخلي أي تحديد المحكمة المختصة للنظر في النزاع وبالتالي تحديد القانون المنطبق، كل ذلك بما يتلاءم وطبيعة الجريمة الإلكترونية.

والجدير بالإشارة في هذا الإطار أن هناك عدة مبادئ تحكم الاختصاص أهمها مبدأ الإقليمية، وهو المبدأ الذي أخذ به **التشريع القطري** بنصه في المادة ١٣ على أنه "تسري أحكام هذا القانون على كل من يرتكب في قطر جريمة من الجرائم المنصوص عليها فيه، وتُعتبر الجريمة مرتكبة في قطر إذا وقع فيها فعل من الأفعال المكونة لها، أو إذا تحققت فيها نتيجتها، أو كان يراد أن تتحقق فيها" [(١)]. أما **المشرع المصري** فقد نظم سريان انطباق أحكام القانون في المكان في المادة ٣.[(٢)]

على أن ذاتية الجرائم الالكترونية قد فرضت على التشريعات الجنائية ضرورة الأخذ بمبدأ تبعي آخر وهو مبدأ الاختصاص العالمي، وهو مبدأ لا يتعارض مع طبيعة قانون العقوبات، لأنه بالأصل هو قانون إقليمي، وهو ليس بعالمي فهو مبدأ احتياطي ثانوي لا يمارس إلا إذا تعذر معاقبة المجرم بدون اللجوء إليه، ولا شك أن مبدأ العالمية الملائم لمعظم الجرائم المعلوماتية لاسيما أن السلوك الإجرامي فيها يتوزع على أكثر من دولة، فالشبكة المعلوماتية عابرة للقارات، تمكن عديد الافراد من الولوج إليها من مناطق مختلفة حول العالم، ما يترتب عنه ضرورة تراجع مبدأ الإقليمية، فهذا الأخير يعاني من بعض القيود بسبب عالمية الإنترنت[(٣)]، لأن من أهم ما يثيره موضوع الجرائم المعلوماتية أن شبكة الإنترنت ليس لها مقر في دولة معينة، ولا تتعلق بشخص محدد، فضلاً على أنها لا تخضع لرقابة أو سيطرة دولة معينة بحد ذاتها، كما أنه لا وجود لقانون جنائي موحد بربطها، فقواعد الإباحة والتجريم تتعدد بتعدد الدول التي ترتبط بهذه الجريمة[(٤)].

---

(١) المادة ١٣ من القانون رقم (١١) لسنة ٢٠٠٤ المتعلق بإصدار قانون العقوبات.

(٢) قانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات.

(٣) إبراهيم العناني، "التعاون الدولي في مواجهة الجريمة الإلكترونية"، مؤتمر التعاون الدولي جريمة إلكترونية الجريمة السيبرانية، الدوحة، ٢٠١٨، ص. ١-١٠.

(٤) حسين بن سعيد، الغافري، السياسية الجنائية في مواجهة جرائم الإنترنت، دار النهضة العربية، القاهرة ٢٠٠٩، ص٥٧٦.

يترتب عما سبق ضرورة إعادة النظر في ترتيب تلك المعاير المحددة للاختصاص وتقديم معيار الدولية، بشكل يصبح معه أن الدولة التي تقع في إقليمها الجريمة أو الجزء الأوفر من النشاط المادي، أو الدولة التي توجد في إقليمها متحصلات الجريمة تكون هي المختصة في مكافحة الجريمة وعقاب مرتكبها. بالتالي، فإن ما سبق كافياً للجزم بذاتية الجريمة الالكترونية على مستوى تطبيق قواعد الاختصاص التي بانت معها أن القواعد التقليدية لا تتناسب مع الجريمة الإلكترونية، فهذه لا تعترف بالحدود الجغرافية للدول، وهذه الذاتية على مستوى الاختصاص انعكست بدورها على ضرورة التعاون الدولي لمكافحة هذا النوع من الجرائم وهو مستوى الذاتية الثاني الذي سيق الحديث عنه.

يعتبر التعاون الدولي أحد أبرز الآليات التي يقع من خلالها مواجهة الجريمة الإلكترونية، وتبرز أهميته من ذاتية الجريمة الإلكترونية باعتبارها جريمة عابرة للحدود، ويبرز دور التعاون الدولي لمكافحة هذا النشاط الإجرامي الدولي، حيث نلاحظ أن المجرم يخطط لسلوكه الإجرامي في بلد معين، ويقوم بتنفيذ الجريمة في بلد آخر، ثم يرحل إلى بلد ثالث فاراً من العدالة، وعليه فإن الجريمة أصبح لها طابع دولي والمجرم أصبح مجرماً دولياً، وهذا ينطبق على الجرائم الإلكترونية حيث يلعب دوراً في مكافحتها عبر التعاون بين الأجهزة التابعة للدول[١] .

كما تعرف المساعدة القضائية الدولية على أنها الإجراء القضائي الذي تقوم به دولة معينة بغية تسهيل مهمة المحاكمة في دولة أخرى بشأن جريمة من الجرائم [٢]، والتي بدورها كانت محط اهتمام التشريع القطري الذي لم يكتف بالأحكام العامة المتعلقة بالتعاون الدولي الواردة في قانون الإجراءات الجنائية، وإنما عمد إلى تعزيزها بأحكام تفصيلية وقع ذكرها صلب قانون مكافحة الجرائم الإلكترونية رقم (١٤) لسنة ٢٠١٤ ، حيث خصص الباب الرابع منه لتنظيم هذا النوع من الإجراءات، وقسمها لفصول ثلاث وهي: القواعد العامة، المساعدة القانونية المتبادلة، تسليم المجرمين.

(١) فهد عبدالله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندرية ٢٠١٦، ص٤٦٣-٤٦٤.

(٢) فهد عبدالله العازمي، مرجع سابق، ص ٤٨١.

الخاتمة

لقد فرضت البنية الخاصة للجرائم المعلوماتية ضرورة وجود نصوص تشريعية خاصة بهذا النوع المستحدث من الجرائم، وهو ما لم يتوانى عنه المشرع القطري الذي سن القانون المنظم للجرائم الإلكترونية والذي بانت فيه ذاتية الجريمة المعلوماتية بالمقارنة مع الجرائم التقليدية الواردة صلب المنظومة الجنائية، وقد اخترنا في سبيل ابراز هذه الذاتية لهذه الجرائم تقسيمها الى ذاتية على مستوى القواعد الموضوعية من جهة والاجرائية من جهة أخرى، رصدنا في حديثنا عما تتمتع به الجريمة المعلوماتية من ذاتية على المستوى الموضوعي خصوصيتها على مستوى التجريم لاسيما من حيث الأركان وما تتطلبه من ركن مفترض يتمثل في البيئة الرقمية فضلاً عن باقي أركان الجريمة وايضاً ما لاحظناه من توسيع في صور الجرائم المعلوماتية ولم تقتصر الذاتية الموضوعية على التجريم بل امتدت لتشمل العقاب الذي اتسم بتنوعه مع أخذ المشرع بعين الاعتبار طبيعة المجرم الإلكتروني الامر الذي حذا به لسن عقوبات تتلاءم وطبيعته وسلوكه الاجرامي.

ثم انتقلنا للحديث عن المستوى الثاني لذاتية الجرائم المعلوماتية على الجانب الاجرائي لاسيما على مستوى الأدلة المعتمدة في اثبات الجريمة المعلوماتية وما تتمتع به من طبيعة خاصة مقارنة مع الأدلة التقليدية، أما المستوى الثاني فكان للحديث عن التحقيق في الجريمة المعلوماتية والذي كشفنا فيه أن إجراءات التحقيق ولئن كانت نفسها المعتمدة في باقي الجرائم الا أنه يقع تطويعها بشكل تراعي فيه خصوصية الجريمة المعلوماتية حتى تصبح الإجراءات العامة للتحقيق ذات نجاعة في الكشف عن الجريمة والقبض على المجرم الإلكتروني تمهيداً لمحاكمته.

<u>وقد توصلنا من خلال هذا البحث لجملة من النتائج المتمثلة في التالي:</u>

١- للجرائم الإلكترونية ذاتية خاصة بها تميزها عن الجرائم التقليدية من حيث الإثبات والتجريم والعقوبة المقررة ومصادرة أدوات الجريمة.

٢- تحتاج الجرائم الإلكترونية تشريعات خاصة تواكب التطور المتسارع للجريمة الإلكترونية .

٣- يلزم لمواجهة الجرائم الجنائية كوادر أمنية وقضائية قادرة على التعامل مع هذا

النوع من الجرائم .

٤- هناك جهود دولية للتعاون في مكافحة الجرائم الإلكترونية ولكنها ليست كافية لمنع الجريمة والحد من ارتكابها أو القبض على الجناة وتسليمهم للمحاكمة.

وقد توصلنا من خلال هذا البحث لجملة من التوصيات المتمثلة في التالي:

١- الحاجة المستمرة لمواكبة التطور التكنولوجي والتطوير الدائم لقانون مكافحة الجرائم الإلكترونية.

٢- بذل المزيد من الجهود في ابرام المعاهدات الثانية والمتعددة في إطار مكافحة الجريمة الالكترونية وذلك من أجل إضفاء مزيد الفاعلية على التعاون الدولي بتسليم المجرمين وتبادل المعارف والمعلومات حول السلوكيات الالكترونية الإجرامية.

٣- تدريب وتأهيل مأموري الضبط القضائي والمحققين على تقنية المعلومات والحاسب الآلي واليات التعامل مع الأدلة الالكترونية والحفاظ عليها لإضفاء مزيد النجاعة على دورهم في مكافحة الجريمة وللحد من الجرائم الإلكترونية.

٤- توسيع رقعة التدريب الالكتروني ليشمل القضاة قصد حسن الفصل في النزاعات المتعلقة بالجرائم الإلكترونية ومواكبتهم للتطور التكنولوجي المستمر، وعدم قصور المامهم بالسلوكيات الاجرامية التقليدية في عصر الثورة المعلوماتية.

قائمة المراجع والمصادر

أولاً: المراجع العامة:

١.غنام محمد غنام، بشير سعد زغلول، شرح قانون العقوبات القطري القسم العام – نظرية الجريمة – نظرية الجزاء، إصدارات كلية القانون –جامعة قطر٢٠١٩.

٢.فرج القصير، القانون الجنائي العام، مركز النشر الجامعي، تونس، ٢٠٠٦.

٣.عمر رمضان، فكرة النتيجة في قانون العقوبات، دار الاسراء للنشر والتوزيع، الأردن ١٩٩٨.

٤.محمد علي السالم الحلبي، شرح قانون العقوبات، دار الثقافة للنشر والتوزيع، عمان ١٩٩٧.

٥.ماجد الزارع، الركن المادي في الجرائم المعلوماتية، أطروحة (ماجستير)-جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجنائية، تخصص التشريع الجنائي الإسلامي، ٢٠١٤.

٦.حازم حسن الجمل، الحماية الجنائية للأمن الإلكتروني، ط١، دار الفكر والقانون، مصر ٢٠١٥.

٧.عبد الفتاح حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة ٢٠٠٧.

٨.عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية، ٢٠١٠.

٩.حسين بن سعيد، الغافري، السياسية الجنائية في مواجهة جرائم الإنترنت، دار النهضة العربية، القاهرة ٢٠٠٩.

١٠.فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندرية ٢٠١٦.

١١.أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية ٢٠١٥.

١٢.محمد كمال الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية: دراسة مقارنة، دار الفكر والقانون للنشر والتوزيع، مصر٢٠١٥.

١٣.علي عدنان الفيل، إجراء التحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، الإسكندرية ٢٠١٢.

١٤.حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، ط١، دار النهضة العربية، القاهرة ٢٠١٧.

١٥.محمد الأمين البشري، التحقيق في الجرائم المستحدثة، ط١، جامعة نايف للعلوم الأمنية، الرياض ٢٠٠٤.

ثانياً: المقالات:

١.محمد علي السالم، الجريمة المعلوماتية، مجلة جامعة بابل، مج١٤ ع ٢، ٢٠١٧ .

٢.علياء القحطاني، الحماية الجنائية من جرائم التعدي على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية، مجلة القانون والأعمال، ع ٧٥، ٢٠٢١.

٣.أحمد عبد المجيد الحاج، المسؤولية الجنائية لجرائم النشر الإلكتروني في ضوء قانون مكافحة جرائم تقنية المعلومات الإماراتي، مجلة الفكر الشرطي، مج٢٢ ع ٨٥، الشارقة ٢٠١٣.

٤.بندر صياح المطيري، جريمة التزوير الإلكتروني في الكويت، مجلة رماح للبحوث والدراسات، ع ٨٨، ديسمبر ٢٠٢٣.

٥.فخري محمود خليل، الأسس القانونية للملكية الفكرية الأدبية والفنية وتطبيقاتها في البيئة الرقمية، الاتحاد العربي للمكتبات، مج ٢، لبنان ٢٠١٠.

٦.طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس ٢٠٠٩.

٧.أسامة العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الأمنية والتدريب م٢٩ ع ٥٨، السعودية ٢٠١٣.

٨.إمام حسنين خليل عطاالله، جرائم الاعتداء على الشبكة المعلوماتية: دراسة تحليلية مقارنة مع التشريع الإماراتي، المجلة الدولية لنشر البحوث والدراسات، مج٢ ع ٨، أبريل ٢٠٢١.

٩.محمد البشري، التحقيق في جرائم الحاسب الآلي والإنترنت، المجلة العربية للدراسات الأمنية، مج ١٥, ع ٣٠، جامعة نايف العربية للعلوم الأمنية، السعودية ٢٠٠٠.

١٠.عبد الحليم بن باردة، إجراءات البحث والتحري عن الجريمة المعلوماتية، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور بالجلفة، الجزائر ٢٠١٥.

١١.إبراهيم العناني، "التعاون الدولي في مواجهة الجريمة الإلكترونية"، مؤتمر التعاون الدولي جريمة إلكترونية الجريمة السيبرانية ، الدوحة، ٢٠١٨.

١٢.محمد عمري، الإثبات الجزائي الإلكتروني في الجرائم المعلوماتية، مجلة العلوم القانونية والسياسية، مج ١٢ ع ٢، العراق ٢٠١٦.

١٣.محمد هلال، كيفية التعامل التقني والأمني مع أوعية الجريمة الرقمية في مسرح الجريمة لضمان حيادة الدليل المستخلص، المجلة العربية الدولية للمعلوماتية، مج٣ ع ٥، جامعة نايف العربية للعلوم الأمنية كلية أمن الحاسب والمعلومات، السعودية ٢٠١٤.

١٤.الحسن بكار، "الطبيعة القانونية للجريمة المعلوماتية،" مجلة الملف، عدد ١٧ (٢٠١٠).

ثالثا: الرسائل والأطروحات:

١.حمد السليطي، تجريم الاحتيال الإلكتروني في القانون المقارن والقطري، مذكرة لنيل شهادة الماجستير، كلية القانون جامعة قطر، قطر٢٠١٨ .

٢.عبد الله القحطاني، تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية: دراسة تطبيقية على المحققين في هيئة الادعاء العام في مدينة الرياض، رسالة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير في قسم العلوم الشرطية، الرياض ٢٠١٤.

٣.نداء المصري، خصوصية الجرائم المعلوماتية، رسالة ماجستير، كلية القانون، جامعة النجاح، نابلس، فلسطين، ٢٠١٧.

٤.عبد الرحمن الدهلاوي، الانتقال والمعاينة في نظم دول مجلس التعاون الخليجي، مذكرة لنيل شهادة الماجستير في العدالة الجنائية، جامعة الإمام محمد بن سعود الإسلامية، السعودية ٢٠٠٨.

رابعاً: الأحكام القضائية القطرية:

١.الحكم الصادر عن محكمة التمييز في الجلسة ١٦-١٠-٢٠١٧، الطعن رقم ٦٠، لسنة ٢٠١٧ محكمة التمييز، المواد الجنائية.

٢.الحكم الصادر عن محكمة التمييز في جلسة ١٦-١٠-٢٠١٧، الطعن رقم ٦٣، لسنة ٢٠١٧ محكمة التمييز، المواد الجنائية .

٣.الحكم الصادر عن محكمة التمييز بجلسة ٠٧-٠١-٢٠١٩، الطعن رقم ١٤٣، لسنة ٢٠١٨ محكمة التمييز، المواد الجنائية.

٤.الحكم الصادر عن محكمة التمييز بجلسة ٢١ من ديسمبر سنة ٢٠٢٠، الطعن رقم ١٦٣ لسنة ٢٠٢٠، تمييز جنائي.

٥.الحكم الصادر عن محكمة التمييز في جلسة ١٨-١٠-٢٠٢١، الطعن رقم ١١١، لسنة ٢٠٢١، المواد الجنائية.

خامساً:المراجع باللغة الأجنبية:

- Digital Evidence: information of probative values stored or transmitted in digital form". Mark M. Pollit, Report on Digital Evidence, presented to 13th Interpol Forensic Science Symposium. Lyon, France, Oct. 162001, 19.

Reference

First: General References

1. Ghannām Muḥammad Ghannām, Bashīr Sa‘d Zaghlūl, sharḥ Qānūn al-‘uqūbāt al-Qaṭarī al-qism al-‘āmm – Naẓarīyat al-jarīmah – Naẓarīyat al-jazā’, Iṣdārāt Kullīyat al-qānūn – Jāmi‘at qṭr2019.
2. Faraj al-Qaṣīr, al-qānūn al-jinā’ī al-‘āmm, Markaz al-Nashr al-Jāmi‘ī, Tūnis, 2006.
3. ‘Umar Ramaḍān, fikrat al-Natījah fī Qānūn al-‘uqūbāt, Dār al-Isrā’ lil-Nashr wa-al-Tawzī‘, al-Urdun 1998.
4. Muḥammad ‘Alī al-Sālim al-Ḥalabī, sharḥ Qānūn al-‘uqūbāt, Dār al-Thaqāfah lil-Nashr wa-al-Tawzī‘, ‘Ammān 1997.
5. Mājid alzār‘, al-Rukn al-māddī fī al-jarā’im al-ma‘lūmātīyah, uṭrūḥat (mājistīr) - jām‘h Nāyif al-‘Arabīyah lil-‘Ulūm al-Amnīyah, Kullīyat al-Dirāsāt al-‘Ulyā, Qism al-‘adālah al-jinā’īyah, takhaṣṣuṣ al-tashrī‘ al-jinā’ī al-Islāmī, 2014.
6. Ḥāzim Ḥasan al-Jamal, al-Ḥimāyah al-jinā’īyah lil-amn al-iliktrūnī, Ṭ1, Dār al-Fikr wa-al-qānūn, Miṣr 2015.
7. ‘Abd al-Fattāḥ Ḥijāzī, Mabādi’ al-ijrā’āt al-jinā’īyah fī Jarā’im al-kumbiyūtar wa-al-Intirnit, Dār al-Kutub al-qānūnīyah, al-Qāhirah 2007.
8. ‘Ā’ishah ibn Qārah Muṣṭafá, Ḥujjīyat al-Dalīl al-iliktrūnī fī majāl al-ithbāt al-jinā’ī fī al-qānūn al-Jazā’irī wa-al-qānūn al-muqāran, Dār al-Jāmi‘ah al-Jadīdah, al-Iskandarīyah, 2010.
9. Ḥusayn ibn Sa‘īd, al-Ghāfirī, al-siyāsīyah al-jinā’īyah fī muwājahat Jarā’im al-intirnit, Dār al-Nahḍah al-‘Arabīyah, al-Qāhirah 2009.
10. Fahd ‘Abd Allāh al-‘Ubayd al-‘Āzimī, al-ijrā’āt al-jinā’īyah al-ma‘lūmātīyah, Dār al-Jāmi‘ah al-Jadīdah, al-Iskandarīyah 2016.
11. Ashraf ‘Abd al-Qādir Qandīl, al-ithbāt al-jinā’ī fī al-jarīmah al-iliktrūnīyah, Dār al-Jāmi‘ah al-Jadīdah, al-Iskandarīyah 2015.
12. Muḥammad Kamāl al-Dasūqī, al-Ḥimāyah al-jinā’īyah lsryh al-ma‘lūmāt al-iliktrūnīyah : dirāsah muqāranah, Dār al-Fikr wa-al-qānūn lil-Nashr wa-al-Tawzī‘, mṣr2015.
13. ‘Alī ‘Adnān al-Fīl, ijrā’ al-taḥqīq al-ibtidā’ī fī al-jarīmah al-ma‘lūmātīyah, al-Maktab al-Jāmi‘ī al-ḥadīth, al-Iskandarīyah 2012.
14. Ḥāzim Muḥammad Ḥanafī, al-Dalīl al-iliktrūnī wa-dawruhu fī al-majāl al-jinā’ī, Ṭ1, Dār al-Nahḍah al-‘Arabīyah, al-Qāhirah 2017.
15. Muḥammad al-Amīn al-Bishrī, al-taḥqīq fī al-jarā’im al-mustaḥdathah, Ṭ1, Jāmi‘at Nāyif lil-‘Ulūm al-Amnīyah, al-Riyāḍ 2004.

Second: Articles

1. Muḥammad ‘Alī al-Sālim, al-jarīmah al-ma‘lūmātīyah, Majallat Jāmi‘at Bābil, mj14 ‘A 2, 2017.
2. ‘Alyā’ al-Qaḥṭānī, al-Ḥimāyah al-jinā’īyah min Jarā’im al-ta‘addī ‘alá anẓimat wa-barāmij wa-shabakāt al-ma‘lūmāt wa-al-mawāqi‘ al-iliktrūnīyah, Majallat al-qānūn wa-al-a‘māl, ‘A 75, 2021.
3. Aḥmad ‘Abd al-Majīd al-Ḥājj, al-Mas’ūlīyah al-jinā’īyah li-jarā’im al-Nashr al-iliktrūnī fī ḍaw’ Qānūn Mukāfaḥat Jarā’im Taqnīyat al-ma‘lūmāt al-Imārātī, Majallat al-Fikr al-sharṭī, mj22 ‘A 85, al-Shāriqah 2013.
4. Bandar Ṣayyāḥ al-Muṭayrī, Jarīmat al-tazwīr al-iliktrūnī fī al-Kuwayt, Majallat Rimāḥ lil-Buḥūth wa-al-Dirāsāt, ‘A 88, Dīsimbir 2023.
5. Fakhrī Maḥmūd Khalīl, al-Usus al-qānūnīyah lil-milkīyah al-fikrīyah al-adabīyah wa-al-fannīyah wa-taṭbīqātuhā fī al-bī’ah al-raqmīyah, al-Ittiḥād al-‘Arabī lil-Maktabāt, Majj 2, Lubnān 2010.
6. Ṭāriq Muḥammad al-Jamalī, al-Dalīl al-raqmī fī majāl al-ithbāt al-jinā’ī, Waraqah ‘amal muqaddimah lil-Mu’tamar al-Maghāribī al-Awwal ḥawla al-ma‘lūmātīyah wa-al-qānūn, Akādīmīyat al-Dirāsāt al-‘Ulyā, Ṭarābulus 2009.
7. Usāmah al-‘Ubaydī, al-taftīsh ‘an al-Dalīl fī al-jarā’im al-ma‘lūmātīyah, al-Majallah al-

‘Arabīyah lil-Dirāsāt al-Amnīyah wa-al-Tadrīb m29 ‘A 58, al-Sa‘ūdīyah 2013.
8. Imām Ḥasanayn Khalīl ‘Aṭāllāh, Jarā’im al-i‘tidā’ ‘alá al-Shabakah al-ma‘lūmātīyah : dirāsah taḥlīlīyah muqāranah ma‘a al-tashrī‘ al-Imārātī, al-Majallah al-Dawlīyah li-Nashr al-Buḥūth wa-al-Dirāsāt, mj2 ‘A 8, Abrīl 2021.
9. Muḥammad al-Bishrī, al-taḥqīq fī Jarā’im al-Ḥāsib al-Ālī wa-al-Intirnit, al-Majallah al-‘Arabīyah lil-Dirāsāt al-Amnīyah, Majj 15, ‘A 30, Jāmi‘at Nāyif al-‘Arabīyah lil-‘Ulūm al-Amnīyah, al-Sa‘ūdīyah 2000.
10. ‘Abd al-Ḥalīm ibn bāridah, Ijrā’āt al-Baḥth wāltḥry ‘an al-jarīmah al-ma‘lūmātīyah, Majallat al-Ḥuqūq wa-al-‘Ulūm al-Insānīyah, Jāmi‘at Zayyān ‘Āshūr bāljlfh, al-Jazā’ir 2015.
11. Ibrāhīm al-‘Anānī, "al-Ta‘āwun al-dawlī fī muwājahat al-jarīmah al-iliktrūnīyah", Mu’tamar al-Ta‘āwun al-dawlī Jarīmat iliktrūnīyah al-jarīmah alsybrānyh, al-Dawḥah, 2018.
12. Muḥammad ‘Umarī, al-ithbāt al-jazā’ī al-iliktrūnī fī al-jarā’im al-ma‘lūmātīyah, Majallat al-‘Ulūm al-qānūnīyah wa-al-siyāsīyah, Majj 12 ‘A 2, al-‘Irāq 2016.
13. Muḥammad Hilāl, kayfīyat al-ta‘āmul al-tiqanī wa-al-amnī ma‘a aw‘yh al-jarīmah al-raqmīyah fī masraḥ al-jarīmah li-Ḍamān ḥyādh al-Dalīl al-Mustakhlaṣ, al-Majallah al-‘Arabīyah al-Dawlīyah lil-Ma‘lūmātīyah, mj3 ‘A 5, Jāmi‘at Nāyif al-‘Arabīyah lil-‘Ulūm al-Amnīyah Kullīyat Amn al-Ḥāsib wa-al-Ma‘lūmāt, al-Sa‘ūdīyah 2014.
14. al-Ḥasan Bakkār, "al-ṭabī‘ah al-qānūnīyah lil-jarīmah al-ma‘lūmātīyah," Majallat al-milaff, ‘adad 17 (2010).

Third: Scientific papers and dissertations

1. Ḥamad al-Sulayṭī, Tajrīm al-iḥtiyāl al-iliktrūnī fī al-qānūn al-muqāran wa-al-Quṭrī, Mudhakkirah li-nayl shahādat al-mājistīr, Kullīyat al-qānūn Jāmi‘at Qaṭar, Qaṭar 2018.
2. ‘Abd Allāh al-Qaḥṭānī, taṭwīr mahārāt al-taḥqīq al-jinā’ī fī muwājahat al-jarā’im al-ma‘lūmātīyah : dirāsah taṭbīqīyah ‘alá al-muḥaqqiqīn fī Hay’at al-iddi‘ā’ al-‘āmm fī Madīnat al-Riyāḍ, Risālat muqaddimah astkmālan li-mutaṭallabāt al-ḥuṣūl ‘alá darajat al-mājistīr fī Qism al-‘Ulūm al-sharṭīyah, al-Riyāḍ 2014.
3. Nidā’ al-Miṣrī, Khuṣūṣīyat al-jarā’im al-ma‘lūmātīyah, Risālat mājistīr, Kullīyat al-qānūn, Jāmi‘at al-Najāḥ, Nābulus, Filasṭīn, 2017.
4. ‘Abd al-Raḥmān aldhlāwy, al-intiqāl wālm‘āynh fī naẓm duwal Majlis al-Ta‘āwun al-Khalījī, Mudhakkirah li-nayl shahādat al-mājistīr fī al-‘adālah al-jinā’īyah, Jāmi‘at al-Imām Muḥammad ibn Sa‘ūd al-Islāmīyah, al-Sa‘ūdīyah 2008.

Fourth: Qatari judicial rulings

1. al-ḥukm al-ṣādir ‘an Maḥkamat al-Tamyīz fī al-jalsah 16-10-2017, al-ṭa‘n raqm 60, li-sanat 2017 Maḥkamat al-Tamyīz, al-mawādd al-jinā’īyah.
2. al-ḥukm al-ṣādir ‘an Maḥkamat al-Tamyīz fī jalsat 16-10-2017, al-ṭa‘n raqm 63, li-sanat 2017 Maḥkamat al-Tamyīz, al-mawādd al-jinā’īyah.
3. al-ḥukm al-ṣādir ‘an Maḥkamat al-Tamyīz bjlsh 07-01-2019, al-ṭa‘n raqm 143, li-sanat 2018 Maḥkamat al-Tamyīz, al-mawādd al-jinā’īyah.
4. al-ḥukm al-ṣādir ‘an Maḥkamat al-Tamyīz bjlsh 21 min Dīsimbir sanat 2020, al-ṭa‘n raqm 163 li-sanat 2020, Tamyīz jinā’ī.
5. al-ḥukm al-ṣādir ‘an Maḥkamat al-Tamyīz fī jalsat 18-10-2021, al-ṭa‘n raqm 111, li-sanat 2021, al-mawādd al-jinā’īyah.

Fifth: References in foreign languages:

- Digital Evidence: information of probative values stored or transmitted in digital form". Mark M. Pollit, Report on Digital Evidence, presented to 13th Interpol Forensic Science Symposium. Lyon, France, Oct. 162001, 19.

فهرس الموضوعات